



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA

Lei n.º 14.133/2021

Contratações de TIC

DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA – DFD			
Órgão: Conselho Regional de Contabilidade do Espírito Santo			
Setor Requisitante (Unidade/Setor/Depto): Setor Administrativo / Dpto de Tecnologia da Informação			
Responsável pela Demanda:	Matrícula:	E-mail:	Telefone:
Wekson José Barbieri Mariano	087	wekson.mariano@crc-es.org.br	27 3232-1610
1. Objeto da Contratação:			
Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.			

2. Justificativa da necessidade da contratação de serviço terceirizado:

2.1. Motivação da Contratação:

O **Conselho Regional de Contabilidade do Espírito Santo (CRCES)** desempenha um papel essencial na sociedade, oferecendo serviços como fiscalização e registro do exercício profissional, orientação técnica e promoção de desenvolvimento profissional da classe contábil. A execução eficiente dessas atividades depende diretamente de uma **infraestrutura de Tecnologia da Informação (TI)** robusta, segura e eficaz, capaz de atender às crescentes demandas internas e externas e garantir a proteção de dados sensíveis, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**.

Atualmente, o CRCES conta com apenas **um servidor técnico especializado em TI**, o qual se encontra sobrecarregado com demandas operacionais, administrativas e técnicas. Essa limitação compromete a execução de atividades críticas e complexas, como:

- Manutenção de servidores e redes;
- Monitoramento contínuo da infraestrutura;
- Gestão de incidentes e mudanças;
- Suporte técnico especializado;
- Implementação de políticas de segurança da informação.

Além disso, a **infraestrutura de rede cabeada apresenta falhas recorrentes**, impactando diretamente a conectividade e a produtividade das equipes. A segurança da informação também requer reforços, com a **adoção de soluções modernas e eficazes contra ameaças cibernéticas**.

Atualmente, o CRCES mantém o **Contrato Administrativo nº 40/2024**, firmado com a empresa Smart Fusion Technology Ltda, com vigência até 15/12/2025. Contudo, trata-se de contrato emergencial, **sem possibilidade de prorrogação**, o que torna **necessária a realização de novo procedimento licitatório**, a fim de garantir a contratação regular e contínua dos serviços especializados de gerenciamento de TI.

A nova contratação tem como objetivo **assegurar a continuidade, eficiência e segurança das operações tecnológicas do CRCES** por meio da prestação dos seguintes serviços especializados:

- Suporte técnico avançado para a infraestrutura tecnológica;
- Manutenção preventiva e corretiva de servidores e redes;
- Gestão de incidentes e implementação de melhorias;
- Monitoramento proativo da infraestrutura de TI;
- Fornecimento, instalação e gestão de **rede Wi-Fi corporativa**;
- Implantação e gestão de **Firewall de Próxima Geração**;
- Implementação e gerenciamento de **solução de backup híbrida** (local e em nuvem), conforme exigências da LGPD.

Além disso, a contratação visa **reduzir a sobrecarga do único servidor de TI**, promovendo maior eficiência e qualidade dos serviços prestados pelo Conselho à sociedade e à classe contábil.

Natureza do Objeto – Serviço Comum e Continuado

O objeto desta contratação caracteriza-se como **serviço comum**, nos termos do inciso II do art. 6º da **Lei nº 14.133/2021**, por poder ser descrito de forma objetiva e padronizada, sem necessidade de especificações técnicas complexas ou qualificações exclusivas. São serviços amplamente ofertados no mercado, com condições técnicas e comerciais similares entre fornecedores.

Trata-se, ainda, de **serviço de natureza continuada**, tendo em vista a sua **necessidade permanente e ininterrupta**, indispensável à execução das atividades finalísticas do CRCES. A descontinuidade desses serviços comprometeria a segurança da informação, a funcionalidade dos sistemas internos e a continuidade do atendimento ao público.

Diante do exposto, justifica-se a abertura de procedimento licitatório para a **contratação regular de serviços comuns e continuados de gerenciamento de TI**, garantindo:

- A continuidade das atividades institucionais do CRCES;
- A observância aos princípios da legalidade, eficiência e economicidade;
- A proteção de dados sensíveis, conforme previsto na LGPD;
- A segurança, estabilidade e evolução da infraestrutura tecnológica do Conselho.

Alinhamento com o Planejamento Estratégico

6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

3. Quantidade de serviço a ser contratada:

- O objeto contempla o **fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa**, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES, conforme CATSER nº **30710**, com vigência de **12 (doze) meses**.
- Inclui-se também a **instalação e gestão de Firewall de Próxima Geração**, de modo a fortalecer a segurança da rede e proteger os dados do CRCES contra ameaças cibernéticas, conforme CATSER nº **30736**, com vigência de **12 (doze) meses**.
- A contratação abrange ainda o **suporte técnico avançado (remoto e presencial)**, destinado à manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, bem como manutenção preventiva e corretiva de todo o parque de TI, conforme CATSER nº **30728**, com vigência de **12 (doze) meses**.
- Por fim, contempla-se a **implementação e gestão de solução de backup local e em nuvem**, assegurando a disponibilidade e integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, medida essencial para a continuidade dos negócios e conformidade com a LGPD, conforme CATSER nº **30744**, com vigência de **12 (doze) meses**.

4. Indicação dos membros da Equipe de Planejamento:

FUNÇÃO/CARGO	NOME DO(A) FUNCIONÁRIO(A)	MATRÍCULA
Integrante-Coordenador da Equipe de Planejamento	Wekson José Barbieri Mariano	87
Integrante	Vanessa Rangel Marques	140
Integrante	Elaine Leopoldino Ferreira	198

5. Responsável pela Formalização da Demanda:

Local e Data:	
Responsável pela Formalização da Demanda: Elaine Leopoldino Ferreira	

6. Responsável pela Autorização da Demanda:

Local e Data:	

Chefia Responsável pela Autorização da Demanda: Walterleno Maifrede Noronha Presidente	

Referência: Processo nº
9079618110000798.000203/2023-73

SEI nº 0142051



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 21/08/2025, às 17:36, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 22/08/2025, às 07:49, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 22/08/2025, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 25/08/2025, às 07:19, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0929590** e o código CRC **96C1B290**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0929590



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

PORTARIA CRCES Nº 042, DE 24 DE MAIO DE 2024

Nomeia os membros da **Comissão de Planejamento das Contratações**, do Conselho Regional de Contabilidade do Espírito Santo - CRCES

O PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE ESPÍRITO SANTO,
no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Portaria CRCES nº 79, de 01 de julho de 2022, que instituiu a Comissão de Planejamento das Contratações do Conselho Regional de Contabilidade do Espírito Santo - CRCES;

CONSIDERANDO a necessidade de recomposição da Comissão;

R E S O L V E:

Art. 1º. Nomear os membros da **Comissão de Planejamento das Contratações**, que passa a ter a seguinte composição:

- a) Elaine Leopoldino Ferreira;
- b) Camila Amorim Santos;
- c) Grazielly Inácio Tartaglia;
- d) Helton Henrique de Carvalho;
- e) Leandra Machado;
- f) Rodrigo dos Santos Sanz;
- g) Vanessa Covre Rangel Marques;
- h) Wekson José Barbieri Mariano.

Art. 2º. Na forma do art. 4º da Portaria CRCES nº 79, de 01 de julho de 2022, as reuniões da Comissão, para elaboração de estudos preliminares e do gerenciamento de riscos dos processos de aquisição/contratação deverão ser realizadas com a participação de, no mínimo, três integrantes, observada ainda a natureza do objeto e os aspectos técnicos a serem discutidos.

Art. 3º. Esta Portaria entra em vigor na data de sua assinatura, revogando-se as disposições em contrário, em especial as Portarias CRCES nºs **081**, de 20 de outubro de 2023.

Contador **Walterleno Maifrede Noronha**
Presidente



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 24/05/2024, às 17:01, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0355496** e o código CRC **370D04AA**.

Referência: Processo nº 9079618110000798.000001/2024-11

SEI nº 0355496



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

TERMO Nº 1/2025/CRCES-ADM/CRCES-DIREX

Processo nº 9079618110000798.000048/2025-57

TERMO DE CIENTIFICAÇÃO

Em conformidade com o disposto no §1º do art. 8º do Decreto nº 11.246, de 27 de outubro de 2022, eu, Elaine Leopoldino Ferreira, ocupante de cargo em comissão neste Conselho Regional de Contabilidade, matrícula nº 198, registro minha ciência quanto à indicação para compor a equipe de planejamento.

Nos termos do que estabelece o art. 10 do Decreto nº 11.246/2022, informo que:

☒ Encontro-me apto para a atribuição a mim conferida

☐ Necessito de treinamento para a atribuição a mim conferida, considerando a especificidade dos serviços objeto do presente processo.

Declaro pleno conhecimento das disposições previstas no Decreto nº 11.246, de 2 de maio de 2023.

Elaine Leopoldino Ferreira

Matrícula 198

Assinado eletronicamente via SEI na data consignada



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 21/08/2025, às 17:36, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

https://sei.cfc.org.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0930145** e o código CRC **CBF61B7D**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0930145



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

TERMO Nº 2/2025/CRCES-ADM/CRCES-DIREX

Processo nº 9079618110000798.000048/2025-57

TERMO DE CIENTIFICAÇÃO

Em conformidade com o previsto no §1º do art. 8º do Decreto nº 11.246, de 27 de outubro de 2022, eu, **Vanessa Covre Rangel Marques**, empregada efetiva deste Conselho Regional de Contabilidade, sob a matrícula nº 140, registro minha cientificação quanto a indicação para membro de equipe de planejamento.

Nos termos do que estabelece o art. 10 do Decreto nº 11.246/2022, informo que:

☒ Encontro-me apto para a atribuição a mim conferida

☐ Necessito de treinamento para a atribuição a mim conferida, considerando a especificidade dos serviços objeto do presente processo.

Declaro pleno conhecimento das disposições previstas no Decreto nº 11.246, de 2 de maio de 2023.

Vanessa Covre Rangel Marques

Assinado eletronicamente via SEI na data consignada



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 22/08/2025, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

https://sei.cfc.org.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0930150** e o código CRC **F1ED8DB1**.



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

TERMO Nº 3/2025/CRCES-ADM/CRCES-DIREX

Processo nº 9079618110000798.000048/2025-57

TERMO DE CIENTIFICAÇÃO

Em conformidade com o previsto no §1º do art. 8º do Decreto nº 11.246, de 27 de outubro de 2022, eu, **Wekson José Barbieri Mariano**, empregado efetivo deste Conselho Regional de Contabilidade, sob a matrícula nº 87, registro minha cientificação quanto a indicação para membro de equipe de planejamento.

Nos termos do que estabelece o art. 10 do Decreto nº 11.246/2022, informo que:

☒ Encontro-me apto para a atribuição a mim conferida

☐ Necessito de treinamento para a atribuição a mim conferida, considerando a especificidade dos serviços objeto do presente processo.

Declaro pleno conhecimento das disposições previstas no Decreto nº 11.246, de 2 de maio de 2023.

Wekson José Barbieri Mariano

Assinado eletronicamente via SEI na data consignada



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 22/08/2025, às 07:49, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

https://sei.cfc.org.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0930153** e o código CRC **64A97D63**.

ESTUDO TÉCNICO PRELIMINAR

Processo nº 9079618110000798.000048/2025-57

ESTUDOS PRELIMINARES

O presente documento visa analisar a viabilidade da presente contratação, bem como levantar os elementos essenciais que servirão para compor o Termo de Referência ou projeto Básico, de forma a melhor atender às necessidades da Administração.

Dados do Processo:

Órgão Responsável pela Contratação:	Conselho Regional de Contabilidade do Espírito Santo.
Objeto:	Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
Nº do Processo Administrativo:	9079618110000798.000048/2025-57

1. Justificativa para a Contratação Conjunta de Serviços de Tecnologia da Informação:

1.1. Introdução

O presente estudo tem como objetivo fundamental apresentar a justificativa técnica e legal para a contratação conjunta de diversos serviços de Tecnologia da Informação (TI) pelo Conselho Regional de Contabilidade do Espírito Santo (CRCES). A decisão por uma contratação unificada, em detrimento da fragmentação em múltiplos contratos, fundamenta-se em princípios basilares da administração pública, notadamente a economicidade, a eficiência, a segurança jurídica e a busca pela solução mais vantajosa para a Administração, em consonância com as diretrizes estabelecidas pela Lei nº 14.133/21.

A infraestrutura de TI do CRCES, conforme detalhado ao longo deste documento, é um pilar essencial para a continuidade e a qualidade dos serviços prestados à sociedade e à classe contábil. A complexidade e a interdependência dos serviços de Wi-Fi corporativo, backup, suporte técnico e firewall demandam uma abordagem integrada para garantir a robustez, a segurança e a disponibilidade dos sistemas críticos. A contratação isolada de cada um desses componentes não apenas eleva os riscos operacionais, mas também compromete a gestão eficiente e a otimização dos recursos públicos.

Este texto abordará os aspectos técnicos e jurídicos que sustentam a opção pela contratação conjunta, destacando os benefícios em termos de economicidade, a mitigação de problemas inerentes à multiplicidade de prestadores de serviços e a conformidade com a legislação vigente, em especial a Lei nº 14.133/2021 e as melhores práticas de contratação de soluções de TI para a Administração Pública.

1.2. Da Necessidade da Contratação e a Interdependência dos Serviços de TI

O Conselho Regional de Contabilidade do Espírito Santo (CRCES) reconhece a Tecnologia da Informação como um elemento estratégico e indispensável para o cumprimento de sua missão institucional. A atual infraestrutura de TI, embora funcional, enfrenta desafios significativos que justificam a presente contratação. Conforme o documento de Estudos Preliminares, o CRCES dispõe de apenas um funcionário técnico especializado em TI, o que resulta em sobrecarga de trabalho e na impossibilidade de atender a todas as demandas operacionais e administrativas complexas, como a manutenção de servidores, gestão de incidentes, monitoramento contínuo de redes, implementação de políticas de segurança da informação e suporte técnico especializado. Adicionalmente, a rede cabeada existente apresenta falhas que impactam diretamente a conectividade e a produtividade da instituição.

A contratação em questão visa suprir essas lacunas e fortalecer a infraestrutura de TI do CRCES, abrangendo os seguintes serviços essenciais e interdependentes:

•**Solução de Acesso via Wi-Fi:** Fundamental para garantir conectividade de alta qualidade e superar as limitações da rede cabeada atual,

promovendo a mobilidade e a eficiência no ambiente de trabalho.

•**Firewall de Próxima Geração:** Crucial para fortalecer a segurança da rede, proteger os dados do CRCES contra ameaças cibernéticas e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

•**Serviços Continuados de Suporte (N1, N2 e N3):** Essenciais para a manutenção da infraestrutura tecnológica, garantia do funcionamento adequado dos sistemas críticos, gestão de incidentes e mudanças, e monitoramento contínuo da infraestrutura.

•**Backup Corporativo (Local e em Nuvem):** Indispensável para assegurar a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, garantindo a continuidade dos negócios e a conformidade com a LGPD.

A natureza desses serviços é intrinsecamente interligada. A eficácia de um sistema de backup, por exemplo, depende diretamente da segurança da rede (Firewall) e da capacidade de suporte técnico para gerenciar eventuais falhas. Da mesma forma, a qualidade da conectividade Wi-Fi impacta a performance de todas as aplicações e serviços que trafegam pela rede. A contratação fragmentada desses serviços, com diferentes prestadores, geraria uma série de desafios e riscos que serão detalhados nas seções seguintes, comprometendo a eficiência e a segurança da infraestrutura de TI do CRCES.

1.3. Arcabouço Legal: A Lei nº 14.133/2021 e os Princípios da Contratação Pública

A Nova Lei de Licitações e Contratos Administrativos, Lei nº 14.133, de 1º de abril de 2021, trouxe inovações significativas para o processo de contratação pública no Brasil, com o objetivo de modernizar, otimizar e tornar mais eficientes as aquisições e contratações realizadas pela Administração Pública. Em seu Art. 5º, a Lei elenca uma série de princípios que devem nortear a aplicação da norma, dentre os quais se destacam a economicidade, a eficiência, o interesse público, o planejamento, a transparência, a segurança jurídica e a vantajosidade. Estes princípios são pilares para a justificativa da contratação conjunta dos serviços de TI.

A Lei nº 14.133/2021, ao contrário da legislação anterior, enfatiza a busca pela solução mais vantajosa para a Administração, que não se restringe apenas ao menor preço, mas considera a relação custo-benefício, a qualidade, a inovação e a sustentabilidade. A contratação conjunta de serviços de TI, quando devidamente justificada, alinha-se perfeitamente a essa premissa, pois permite uma visão sistêmica e integrada da infraestrutura, otimizando recursos e minimizando riscos.

Embora a Lei nº 14.133/2021 defina a 'contratação integrada' especificamente para obras e serviços de engenharia (Art. 6º, XXXII), o conceito subjacente de agrupar itens interdependentes para obter maior eficiência e vantajosidade pode ser analogicamente aplicado à contratação de serviços de TI. A Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que disciplina as contratações de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades do SISP, reforça a importância do planejamento e da busca por soluções que atendam às necessidades de forma abrangente e eficiente.

O Estudo Técnico Preliminar (ETP), conforme previsto na Lei nº 14.133/2021 e detalhado na IN SGD/ME Nº 94/2022, é o documento fundamental que embasa a decisão pela contratação. Ele deve contemplar a análise comparativa de soluções e custos, a estimativa do custo total da

contratação e a declaração da viabilidade da contratação. A presente justificativa, ao demonstrar os benefícios da contratação conjunta, serve como subsídio para o ETP, evidenciando que a opção por um único prestador para os serviços de Wi-Fi, backup, suporte e firewall é a que melhor atende aos princípios da Lei e às necessidades do CRCES.

Outro ponto relevante é a Matriz de Alocação de Riscos, que se torna ainda mais crucial em contratações complexas como a de serviços de TI. A Lei nº 14.133/2021 exige a definição clara de riscos e responsabilidades entre as partes. Em uma contratação conjunta, a alocação de riscos é simplificada, pois a responsabilidade pela integração e funcionamento dos diversos componentes recai sobre um único fornecedor, facilitando a gestão e a resolução de eventuais problemas.

1.4. Economicidade e Vantagens da Contratação Conjunta

A busca pela economicidade é um dos princípios fundamentais que regem as contratações públicas, conforme expresso no Art. 5º da Lei nº 14.133/2021. A contratação conjunta dos serviços de TI, em vez de licitações separadas para cada item (Wi-Fi, backup, suporte e firewall), representa uma estratégia que maximiza a eficiência na aplicação dos recursos públicos e gera uma série de vantagens econômicas e operacionais para o CRCES.

Primeiramente, a contratação de um único fornecedor para a gestão integrada de múltiplos serviços de TI permite a obtenção de economias de escala. Ao consolidar a demanda, o CRCES ganha maior poder de negociação, o que pode resultar em propostas mais competitivas e preços unitários mais vantajosos para cada serviço. A diluição de custos administrativos e operacionais do fornecedor em um contrato de maior escopo tende a refletir em um custo total da contratação mais baixo para a Administração Pública.

Além disso, a contratação conjunta simplifica os processos administrativos e burocráticos. A gestão de um único contrato, em comparação com a gestão de múltiplos contratos, reduz significativamente a carga de trabalho da equipe interna do CRCES, liberando recursos humanos para outras atividades estratégicas. Isso se traduz em economia de tempo e, consequentemente, de recursos financeiros, uma vez que menos horas de trabalho são dedicadas à fiscalização e acompanhamento de diversos contratos.

A otimização dos recursos também se manifesta na redução de custos indiretos. A coordenação entre diferentes fornecedores, a resolução de conflitos de responsabilidade e a necessidade de interface entre sistemas distintos geram custos ocultos e ineficiências. Com um único prestador, esses custos são minimizados, pois a responsabilidade pela integração e pelo funcionamento harmonioso de toda a infraestrutura de TI recai sobre uma única empresa, que possui o conhecimento global do ambiente e a capacidade de gerenciar as interdependências de forma proativa.

Por fim, a contratação conjunta contribui para a previsibilidade orçamentária. Com um contrato abrangente, o CRCES tem uma visão mais clara e consolidada dos custos totais envolvidos na manutenção e gestão de sua infraestrutura de TI, facilitando o planejamento financeiro e a alocação de recursos de forma mais eficiente ao longo do tempo. Essa previsibilidade é essencial para uma gestão pública responsável e transparente.

1.5. Mitigação de Problemas e Impactos Negativos da Multiplicidade de Prestadores

A contratação fragmentada de serviços de Tecnologia da Informação, com a pulverização de responsabilidades entre múltiplos prestadores, embora possa parecer, à primeira vista, uma estratégia de diversificação, acarreta uma série de problemas e impactos negativos que comprometem a eficiência, a segurança e a continuidade das operações do CRCES. A experiência demonstra que a gestão de diversos contratos para serviços interdependentes de TI pode gerar complexidades e vulnerabilidades que superam quaisquer supostas vantagens.

Um dos principais desafios reside na incompatibilidade e nas falhas de integração entre os diferentes sistemas e equipamentos fornecidos por empresas distintas. A infraestrutura de TI do CRCES, conforme descrito, é híbrida e complexa, envolvendo soluções de Wi-Fi, backup, suporte e firewall, além de infraestrutura hiperconvergente, acessos VDI, máquinas virtuais e desktops físicos. A falta de um gerenciamento unificado pode levar a problemas de interoperabilidade, dificultando a comunicação entre os componentes e resultando em falhas operacionais, interrupções de serviço e degradação da performance geral do ambiente. A identificação da causa raiz de um problema torna-se um processo moroso e dispendioso, pois cada fornecedor pode atribuir a falha ao outro, criando um cenário de “empurra-empurra” de responsabilidades.

A dificuldade na gestão e fiscalização contratual é outro impacto negativo significativo. A multiplicidade de contratos implica na necessidade de gerenciar diferentes prazos, escopos, níveis de serviço (SLAs) e pontos de contato. Isso sobrecarrega a equipe interna do CRCES, que já é reduzida, desviando seu foco de atividades estratégicas para a burocracia administrativa. A fiscalização torna-se mais complexa, exigindo um esforço desproporcional para garantir que cada fornecedor esteja cumprindo suas obrigações de forma isolada, sem uma visão integrada do impacto no ambiente como um todo.

A diluição da responsabilidade é um risco inerente à contratação fragmentada. Em caso de incidentes de segurança, falhas de sistema ou perda de dados, a apuração do responsável pela falha e a consequente aplicação de sanções contratuais tornam-se extremamente difíceis. Essa incerteza jurídica pode atrasar a resolução de problemas críticos, gerar prejuízos financeiros e de imagem para o CRCES, e comprometer a conformidade com regulamentações como a LGPD. Com um único prestador, a responsabilidade pela integridade e funcionamento de toda a infraestrutura é centralizada, facilitando a governança e a responsabilização.

Adicionalmente, a fragmentação pode levar a custos elevados e ineficiências operacionais. A ausência de uma visão consolidada da infraestrutura impede a otimização de recursos e a identificação de redundâncias ou gargalos. Cada fornecedor pode operar de forma isolada, sem considerar o impacto de suas ações no ambiente geral, o que pode resultar em investimentos desnecessários ou na subutilização de ativos. A falta de padronização e a necessidade de múltiplas interfaces de comunicação entre os fornecedores também contribuem para o aumento dos custos operacionais.

Por fim, a vulnerabilidade de segurança é amplificada em um ambiente com múltiplos prestadores. A gestão de segurança da informação exige uma abordagem holística e integrada. A fragmentação pode criar brechas e pontos cegos, dificultando a implementação de políticas de segurança consistentes e a resposta rápida a ameaças cibernéticas. Um único fornecedor, com uma visão abrangente da infraestrutura, está em melhor posição para implementar e gerenciar soluções de segurança de forma eficaz, garantindo a proteção dos dados e sistemas do CRCES.

Diante desses riscos e impactos negativos, a contratação conjunta de serviços de TI emerge como a solução mais prudente e vantajosa para o CRCES, garantindo a sinergia entre os serviços, a otimização da gestão, a clareza na alocação de responsabilidades e a segurança da infraestrutura tecnológica.

1.6. Conclusão

Diante do exposto, a contratação conjunta dos serviços de Tecnologia da Informação para o Conselho Regional de Contabilidade do Espírito Santo (CRCES), abrangendo Wi-Fi corporativo, backup, serviços de suporte e firewall, configura-se como a abordagem mais estratégica, eficiente e em conformidade com os preceitos da Lei nº 14.133/2021. Esta modalidade de contratação não apenas otimiza a aplicação dos recursos públicos, mas também mitiga os riscos inerentes à fragmentação de serviços interdependentes, garantindo a continuidade, a segurança e a qualidade da infraestrutura de TI do órgão.

A centralização da responsabilidade em um único prestador de serviços especializados em TI proporciona uma gestão mais simplificada e eficaz, com clareza na alocação de responsabilidades e maior agilidade na resolução de problemas. A economicidade é alcançada por meio de ganhos de escala, redução de custos administrativos e operacionais, e maior previsibilidade orçamentária. Adicionalmente, a abordagem integrada fortalece a segurança da informação, minimizando vulnerabilidades e garantindo a conformidade com a legislação vigente, como a LGPD.

Em suma, a contratação conjunta é a solução que melhor atende ao interesse público, promovendo a eficiência, a economicidade e a segurança jurídica, pilares da boa gestão pública. Recomenda-se, portanto, a continuidade do processo licitatório sob esta perspectiva integrada, visando a obtenção da proposta mais vantajosa e a garantia de uma infraestrutura de TI robusta e confiável para o CRCES.

2. Diretrizes gerais para a contratação:

2.1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERADO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INT PÙBLICO;

O **Conselho Regional de Contabilidade do Espírito Santo (CRCES)** desempenha um papel essencial na sociedade, oferecendo serviços como fiscalização e registro do exercício profissional, orientação técnica e promoção de desenvolvimento profissional da classe contábil. A execução eficiente dessas atividades depende diretamente de uma **infraestrutura de Tecnologia da Informação (TI)** robusta, segura e eficaz, capaz de atender às crescentes demandas internas e externas e garantir a proteção de dados sensíveis, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**.

Atualmente, o CRCES conta com apenas **um servidor técnico especializado em TI**, o qual se encontra sobrecarregado com demandas operacionais, administrativas e técnicas. Essa limitação compromete a execução de atividades críticas e complexas, como:

- Manutenção de servidores e redes;
- Monitoramento contínuo da infraestrutura;
- Gestão de incidentes e mudanças;
- Suporte técnico especializado;
- Implementação de políticas de segurança da informação.

Além disso, a **infraestrutura de rede cabeada apresenta falhas recorrentes**, impactando diretamente a conectividade e a produtividade das equipes. A segurança da informação também requer reforços, com a **adoção de soluções modernas e eficazes contra ameaças cibernéticas**.

Atualmente, o CRCES mantém o **Contrato Administrativo nº 40/2024**, firmado com a empresa Smart Fusion Technology Ltda, com vigência até 15/12/2025. Contudo, trata-se de contrato emergencial, **sem possibilidade de prorrogação**, o que torna **necessária a realização de novo procedimento licitatório**, a fim de garantir a contratação regular e contínua dos serviços especializados de gerenciamento de TI.

A nova contratação tem como objetivo **assegurar a continuidade, eficiência e segurança das operações tecnológicas do CRCES**, por meio da prestação dos seguintes serviços especializados:

- Suporte técnico avançado para a infraestrutura tecnológica;
- Manutenção preventiva e corretiva de servidores e redes;
- Gestão de incidentes e implementação de melhorias;
- Monitoramento proativo da infraestrutura de TI;

- Fornecimento, instalação e gestão de **rede Wi-Fi corporativa**;
- Implantação e gestão de **Firewall de Próxima Geração**;
- Implementação e gerenciamento de **solução de backup híbrida** (local e em nuvem), conforme exigências da LGPD.

Além disso, a contratação visa **reduzir a sobrecarga do único servidor de TI**, promovendo maior eficiência e qualidade dos serviços prestados pelo Conselho à sociedade e à classe contábil.

Natureza do Objeto – Serviço Comum e Continuado

O objeto desta contratação caracteriza-se como **serviço comum**, nos termos do inciso II do art. 6º da **Lei nº 14.133/2021**, por poder ser descrito de forma objetiva e padronizada, sem necessidade de especificações técnicas complexas ou qualificações exclusivas. São serviços amplamente ofertados no mercado, com condições técnicas e comerciais similares entre fornecedores.

Trata-se, ainda, de **serviço de natureza continuada**, tendo em vista a sua **necessidade permanente e ininterrupta**, indispensável à execução das atividades finalísticas do CRCES. A descontinuidade desses serviços comprometeria a segurança da informação, a funcionalidade dos sistemas internos e a continuidade do atendimento ao público.

Diante do exposto, justifica-se a abertura de procedimento licitatório para a **contratação regular de serviços comuns e continuados de gerenciamento de TI**, garantindo:

- A continuidade das atividades institucionais do CRCES;
- A observância aos princípios da legalidade, eficiência e economicidade;
- A proteção de dados sensíveis, conforme previsto na LGPD;
- A segurança, estabilidade e evolução da infraestrutura tecnológica do Conselho

2.1.1 – JUSTIFICATIVA PARA CONTRATAÇÃO CONJUNTA DOS SERVIÇOS

2.2 - PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

A contratação possui previsão no Plano de Contratações Anual do CRCES para o exercício 2026, e no Plano Diretor de Tecnologia da Informação.

2.3 - REQUISITOS DA CONTRATAÇÃO

		ITEM 1			
SUBITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

2.2.1 A Contratada deverá prestar **serviços gerenciados de Tecnologia da Informação** que abrangem o **suporte técnico avançado** (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a **gestão de incidentes e mudanças**. O escopo prevê a **gestão completa da infraestrutura de redes** (LAN, VLAN e WLAN), com o **fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa**, e a **gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais**. Será responsável também pelo **monitoramento contínuo da infraestrutura**, com identificação e mitigação proativa de riscos, pela **manutenção preventiva e corretiva** de todo o parque de TI, pela **gestão e monitoramento dos links de internet**, pela **gestão e manutenção da infraestrutura hiperconvergente** e do **banco de dados em SQL Server**. Além disso, inclui o **fornecimento, instalação e gestão de um Firewall de Próxima Geração** e a **implementação e gestão de solução de backup local e em nuvem**. Os serviços atenderão a única localidade do CRCES, até **60 estações de trabalho** (físicas ou virtuais), **5 servidores físicos** e **12 servidores virtuais**.

2.2.2 A empresa contratada deverá estar plenamente capacitada para **gerenciar toda a estrutura de TI híbrida do CRCES**. Esta estrutura é complexa e inclui uma infraestrutura hiperconvergente (sem armazenamento baseado em Software-defined Storage - SDS), uma infraestrutura

complexa e inclui uma **infraestrutura hiperconvergente** (com armazenamento baseado em software-defined storage - SDS), uma **infraestrutura com acessos VDI (Virtual Desktop Infrastructure)** máquinas virtuais e uma **infraestrutura tradicional** (com desktops físicos e notebooks). A Contratada será responsável por assegurar a **gestão completa dos backups e restores** de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a **disponibilidade e integridade dos dados** em todas as plataformas.

2.4 CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS

2.4.1. SOLUÇÃO DE ACESSO VIA WI-FI.

2.4.1.1. Características da solução.

2.4.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

2.4.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

2.4.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

2.4.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

2.4.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

2.4.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

2.4.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.4.1.1.8. Site Survey Preliminar

Para a definição da quantidade de **equipamentos** necessários, conforme detalhado no item 2.4.1.1.2, o CRCES realizou um **levantamento de campo (site survey)** preliminar, cujos resultados são apresentados a seguir:

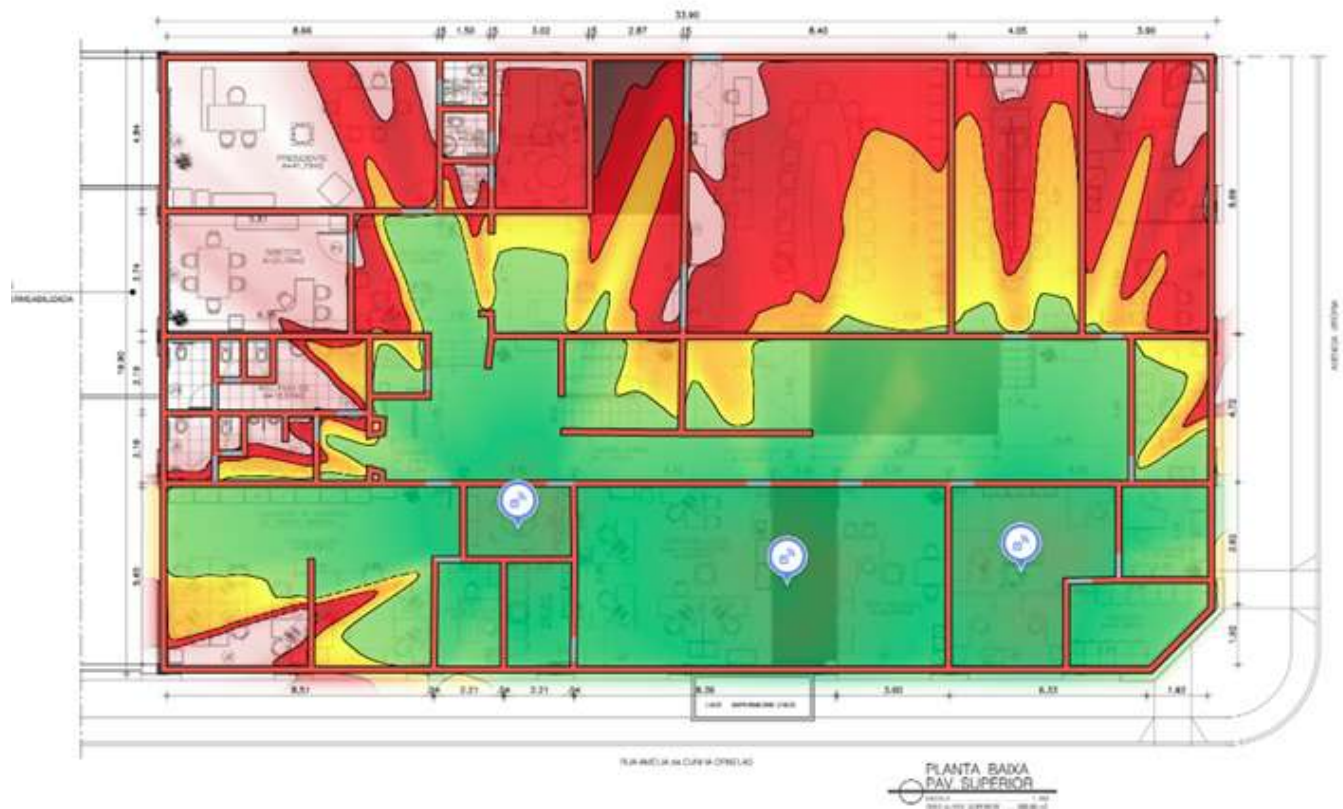
a) Pavimento térreo - 09 equipamentos

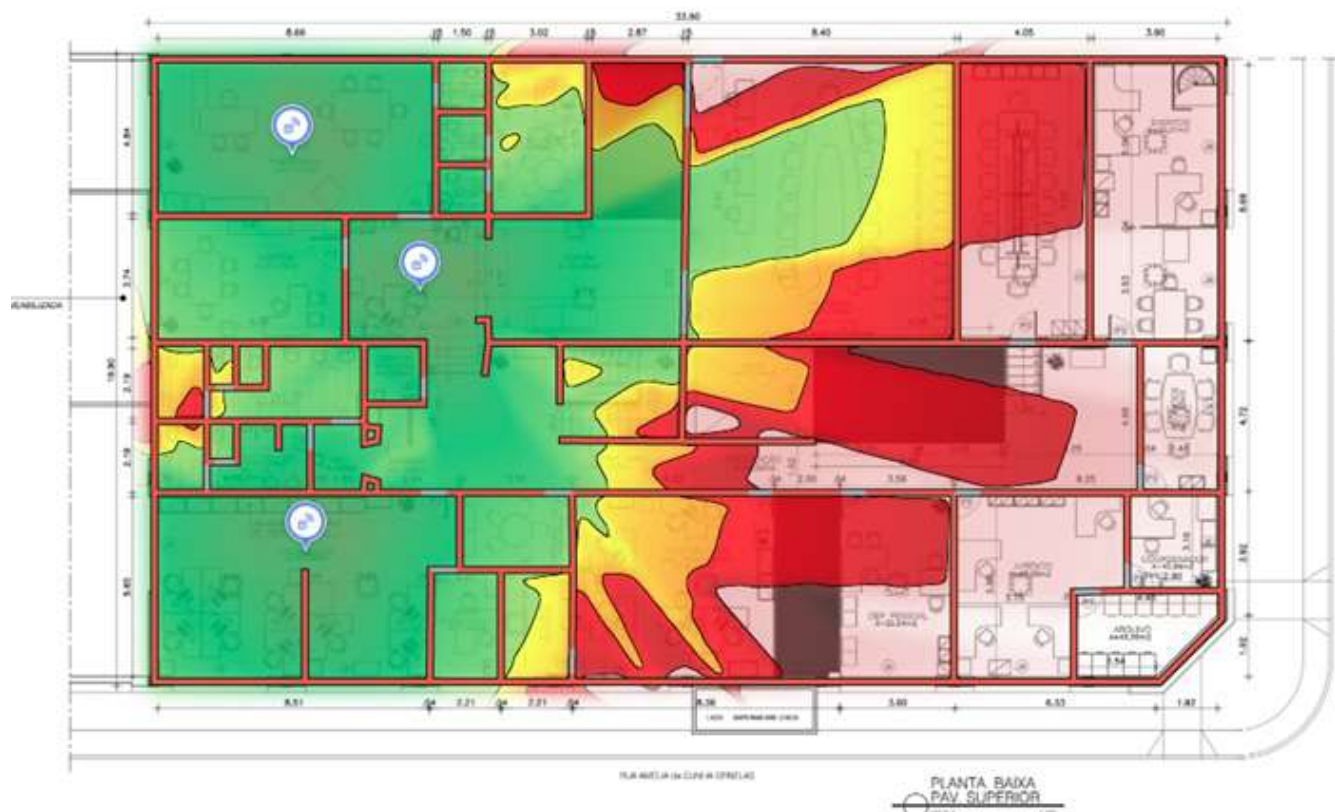




b) Pavimento superior - 09 equipamentos







1.2. Características dos pontos de acesso à internet via Wifi.

1.2.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

1.2.2. Deve ser compatível e gerenciado pelo ITENS "Firewall de Próxima Geração (NGFW) – Tipo 0x" deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

1.2.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

1.2.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

1.2.5. Deve permitir ser gerenciado remotamente através de links WAN;

1.2.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

1.2.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

1.2.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

1.2.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

1.2.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

1.2.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

1.2.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

1.2.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

1.2.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3au;

1.2.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

1.2.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

1.2.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

1.2.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

1.2.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

1.2.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

1.2.20. Deve permitir operação em modo Mesh;

1.2.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

1.2.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

1.2.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

1.2.24. Deve suportar OFDMA;

1.2.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;

1.2.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

1.2.27. Deve suportar BSS Coloring;

1.2.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

1.2.29. Deve suportar operação em 6GHz com canais de 20, 40,80 e 160MHz;

1.2.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);

1.2.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;

1.2.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;

1.2.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

1.2.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

1.2.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

1.2.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

1.2.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);

1.2.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

1.2.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

1.2.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

1.2.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

1.2.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

1.2.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

1.2.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

1.2.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

1.2.46. Deve implementar o padrão IEEE 802.11e;

1.2.47. Deve implementar o padrão IEEE 802.11h;

1.2.48. Deve implementar o padrão IEEE 802.3az;

1.2.49. Deve suportar ser gerenciado via SNMP;

1.2.50. Deve suportar consultas via REST API;

1.2.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

- 1.2.52.** Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;
- 1.2.53.** Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- 1.2.54.** Deve possuir indicadores luminosos (LED) para indicação de status;
- 1.2.55.** O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 1.2.56.** Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 1.2.57.** Deve possuir certificado emitido pela Wi-Fi Alliance;
- 1.2.58.** Deve estar homologado pela ANATEL na data de execução do pregão;
- 1.2.59.** Deve ser licenciado para uso pelo período de duração da contratação.
- 1.2.60.** Deve possuir garantia para uso pelo período de duração da contratação.
- 1.2.61.** Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

1.3. Características do equipamento controlador de pontos de acesso Wifi;

- 1.3.1.** Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 1.3.2.** Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
- 1.3.3.** Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- 1.3.4.** Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
- 1.3.5.** Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 1.3.6.** Deve possuir 1 (uma) interface USB;
- 1.3.7.** Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);
- 1.3.8.** Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 1.3.9.** Deve possuir tabela MAC com suporte a 32.000 endereços;
- 1.3.10.** Deve operar com latência igual ou inferior à 1us (microsegundo);
- 1.3.11.** Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 1.3.12.** Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- 1.3.13.** Deve suportar a comutação de Jumbo Frames;
- 1.3.14.** Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- 1.3.15.** Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- 1.3.16.** Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 1.3.17.** Deve implementar serviço de DHCP Relay;
- 1.3.18.** Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- 1.3.19.** Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 1.3.20.** Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;
- 1.3.21.** Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 1.3.22.** Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 1.3.23.** Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- 1.3.24.** Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
- 1.3.25.** Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 1.3.26.** Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 1.3.27.** Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN

ID;

- 1.3.28.** Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- 1.3.29.** Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 1.3.30.** Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;
- 1.3.31.** Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 1.3.32.** Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 1.3.33.** Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 1.3.34.** Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
- 1.3.35.** Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
- 1.3.36.** Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- 1.3.37.** Deve suportar MAC Authentication Bypass (MAB);
- 1.3.38.** Deve implementar RADIUS CoA (Change of Authorization);
- 1.3.39.** Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 1.3.40.** Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 1.3.41.** Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
- 1.3.42.** Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 1.3.43.** Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 1.3.44.** Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 1.3.45.** Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 1.3.46.** Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 1.3.47.** Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 1.3.48.** Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 1.3.49.** Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 1.3.50.** Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 1.3.51.** Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 1.3.52.** Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 1.3.53.** Deve permitir ser gerenciado através de IPv6;
- 1.3.54.** Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 1.3.55.** Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 1.3.56.** Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 1.3.57.** Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 1.3.58.** Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 1.3.59.** Deverá suportar ser configurado e monitorado através de REST API;
- 1.3.60.** Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 1.3.61.** Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 1.3.62.** Deve suportar temperatura de operação de até 45º Celsius;
- 1.3.63.** Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 1.3.64.** Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 1.3.65.** Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 1.3.66.** Deve ser licenciado para uso pelo período de duração da contratação.
- 1.3.67.** Deve possuir garantia para uso pelo período de duração da contratação.
- 1.3.68.** Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

1.4. Requisitos da instalação dos pontos de acesso à internet via Wifi.

1.4.1. Requisitos para instalação do item 1.2

1.4.2. Serviço de Implementação para rede WLAN

1.4.3. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura 3 total, sendo observada a quantidade mínima estabelecida pela DTIC.

1.4.4. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;

1.4.5. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;

1.4.6. Requisitos gerais de Implantação

1.4.7. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.

1.4.8. Instalação física

1.4.9. Será realizada instalação física conforme a necessidade da contratante.

1.4.10. O ponto de acesso wifi deverá ser fixado no teto ou parede.

1.4.11. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

1.5. Implementação lógica

1.5.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir

1.5.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

1.5.3. Cadastro das subscrições dos APs na plataforma de gerência;

1.5.4. Endereçamento e segmentação das Redes WIRELESS;

1.5.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless);

1.5.6. Definição de políticas de bloqueio e permissão de acesso;

1.5.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;

1.5.8. Configuração de Endereços/Interfaces de Gerência:

1.5.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),

1.5.10. Parâmetros SNMP para monitoração/gerência remota;

1.5.11. Configuração de Syslog, quando aplicável;

1.5.12. Configuração de redes locais (VLANs);

1.5.13. Configuração de redes locais (SSIDs);

1.5.14. Configuração de sincronismo de hora NTP ou SNTP;

1.5.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.

1.5.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;

1.5.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;

1.5.18. Configurações de grupos de ponto de acesso;

1.5.19. Configuração de algoritmo de criptografia a ser utilizado;

1.5.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;

1.5.21. Identificar os pontos de acesso por localização conforme survey realizado;

1.5.22. Configuração de segurança de rede;

1.5.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;

1.5.24. Adequar o posicionamento de pontos de acesso da solução instalada;

1.5.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;

1.5.26. Emissão de relatórios de implantação contendo:

1.5.27. Mapas de rede,

1.5.28. Relação de equipamentos implantados,

1.5.29. Configurações feitas nos softwares;

1.5.30. Resultado dos testes realizados;

1.6. Requisitos para instalação do controlador de pontos de acesso Wifi

- 1.6.1.** Todo o processo de instalação será precedido de um estudo e entendimento de toda a infraestrutura em funcionamento hoje no ambiente englobando sua topologia, todas as configurações em uso (endereçamentos IP, VLANs, rotas, QoS, ACL's, etc),
- 1.6.2.** Para a implementação da solução bem como acompanhamento do projeto proposto, a licitante deverá apresentar profissionais certificados, níveis avançados de conhecimento nas tecnologias ofertados e necessárias para implantação da solução proposta.
- 1.6.3.** O serviço de instalação, configuração da rede precederá de um cronograma de projeto para implementação das ações abaixo descritas, a ser elaborado de comum acordo.
- 1.6.4.** Todo serviço deverá ser realizado por profissional do fabricante ou certificado por ele para execução dos serviços, para isso deverá ser apresentado junto com a proposta o certificado do profissional que irá executar os serviços de implantação
- 1.6.5.** Planejamento e Projeto para Instalação da Solução
- 1.6.6.** Levantamento e análise da configuração atual da rede;
- 1.6.7.** Elaboração de Projeto de Rede detalhado em conjunto com a equipe de tecnologia da informação, incluindo os itens de configuração a seguir:
- 1.6.8.** Endereçamento e segmentação das Redes LAN e WAN;
- 1.6.9.** Roteamento estativo e dinâmico utilizando protocolos RIPv2 e OSPFv2, se aplicável;
- 1.6.10.** Qualidade de Serviço (QoS): regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede;
- 1.6.11. Segurança:**
- 1.6.12.** Dos ativos: protocolos de comunicação segura, autenticação para acesso e proteção contra ataques;
- 1.6.13.** Da rede: controles a serem implementados para restringir o acesso à rede e reduzir a exposição dos servidores e estações de trabalho;
- 1.6.14. Instalação da Solução**
- 1.6.15.** Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;
- 1.6.16.** Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;
- 1.6.17.** Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 1.6.18.** Configuração de Endereços/Interfaces de Gerência;
- 1.6.19.** Endereçamento IP;
- 1.6.20.** Telnet, se necessário;
- 1.6.21.** Secure Shell (SSH), se necessário;
- 1.6.22.** Web (HTTP), se necessário;
- 1.6.23.** Restrições (Filtros/ACLs) de Acesso;
- 1.6.24.** Autenticação;
- 1.6.25.** Parâmetros SNMP para monitoração/gerência remota;
- 1.6.26.** Configuração de redes locais (VLANs);
- 1.6.27.** Configuração de sincronismo de hora NTP ou SNTP;
- 1.6.28.** Configuração do protocolo Rapid Spanning Tree (RSTP);
- 1.6.29.** Configuração de BPDU GUARD;
- 1.6.30.** Configuração de Root Spanning Tree;
- 1.6.31.** Interfaces de roteamento IP;
- 1.6.32.** Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;
- 1.6.33.** Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;
- 1.6.34.** Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 1.6.35. Otimização da Solução**
- 1.6.36.** Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.
- 1.6.37.** Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 1.6.38.** Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;
- 1.6.39.** Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto
- 1.6.40.** Ativação de recursos para o controle de broadcast storms;
- 1.6.41.** Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 1.6.42.** Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 1.6.43.** Controle de acesso a rede através do padrão IEEE 802.1x;
- 1.6.44.** Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;
- 1.6.45.** Configuração de DHCP Snooping;
- 1.6.46.** Configuração de DHCP Relay;
- 1.6.47.** Configuração de interface confiável (trust Interface);
- 1.6.48.** Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.

- 1.6.49. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;
- 1.6.50. Criação e ativação de regras de acesso e perfis de acesso à rede;
- 1.6.51. Configuração de parâmetros de qualidade de serviço (QoS);
- 1.6.52. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;
- 1.6.53. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;
- 1.6.54. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;
- 1.6.55. Ativação e teste das ACLs nos equipamentos fornecidos;

1.6.56. Homologação

- 1.6.57. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.
- 1.6.58. Documentação em formato PDF contendo os itens a seguir:
- 1.6.59. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.
- 1.6.60. Arquivos de configuração dos ativos de rede;
- 1.6.61. Backup das configurações dos softwares utilizados;
- 1.6.62. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega;

1.7. Requisitos para instalação do cabeamento

- 1.7.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;
- 1.7.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;
- 1.7.3. Conectorização e crimpagem dos cabos em ambos os extremos;
- 1.7.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;
- 1.7.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;
- 1.7.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;
- 1.7.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;
- 1.7.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

1.8. Descrição do suporte continuado

- 1.8.1. A CONTRATADA deverá prestar assistência em horário comercial, das 07:30 às 16:30h na modalidade 8x5;
- 1.8.2. A CONTRATADA deverá providenciar a imediata reposição de equipamentos que estejam indisponíveis, seja por manutenção preventiva, seja por manutenção corretiva, avarias, acidentes ou paralisados por falhas provocadas por falta de suprimento, no prazo máximo de 24 (vinte e quatro) horas;
- 1.8.3. Da Manutenção Preventiva A Contratada é a única e exclusiva responsável pela manutenção preventiva dos equipamentos objeto desta contratação; A manutenção deve obedecer às recomendações do fabricante de cada equipamento, porém, sem se limitar a elas e aos serviços abaixo descritos:
- 1.8.4. Providenciar revisão geral de todos os itens previstos de acordo com a recomendação do fabricante;
- 1.8.5. Verificar o estado geral de conservação dos equipamentos e providenciar substituição dos mesmos sempre que for necessário;
- 1.8.6. Efetuar as revisões periódicas, observando as recomendações do fabricante;
- 1.8.7. A Contratada deverá realizar as manutenções preventivas para garantir o pleno funcionamento dos equipamentos e a qualidade dos materiais produzidos.

1.8.8. Manutenção Corretiva

- 1.8.9. A manutenção corretiva deverá ocorrer sempre que a substituição do equipamento for necessária por quebra, assim como quando surgirem falhas;
- 1.8.10. A CONTRATADA deverá iniciar a manutenção corretiva em um prazo máximo de 4 (quatro) horas após a notificação por parte da CONTRATANTE, respeitando os horários definidos pela CONTRATANTE para essa tarefa;
- 1.8.11. A CONTRATADA deverá arcar com todos os custos decorrentes de avarias, exceto os decorrentes do mau uso do equipamento por parte do Contratante; Nesses casos, será de responsabilidade do Contratante arcar com os custos de reparo do equipamento;
- 1.8.12. A CONTRATADA deverá assumir integral e absoluta responsabilidade pelos equipamentos locados, desobrigando a CONTRATANTE de qualquer ônus, encargos, deveres e responsabilidade por defeitos, vícios aparentes ou ocultos, ou funcionamento insatisfatório dos aludidos bens e acidentes.

1.8.13. Serviço continuado

- 1.8.14. CONTRATADA deverá assumir a responsabilidade pelo gerenciamento da WLAN no que tange as seguintes ações:
- 1.8.15. Provisionamento e descoberta de dispositivos;
- 1.8.16. Prestar suporte técnico remoto e presencial;
- 1.8.17. Realizar atualizações de firmware e patches de segurança nos equipamentos;
- 1.8.18. Fazer a gestão de capacidade, espectro e canais da rede wireless;
- 1.8.19. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 1.8.20. Monitorar continuamente a saúde dos dispositivos
- 1.8.21. Monitorar perfil de usuário;

- 1.8.22.** Monitorar Autenticação de usuários;
- 1.8.23.** Proteção e implementação de WLAN usando os protocolos de segurança descritos no TR;
- 1.8.24.** Entregar relatórios mensais com análise de disponibilidade, uso de canais, desempenho e incidentes;
- 1.8.25.** Substituir equipamentos com defeito conforme cláusulas de SLA;
- 1.8.26.** Corrigir falhas em conectores, cabos, patch panels e pontos RJ45 usados na solução;

2. ITEM - FIREWALL (SEDE)

2.1. Características da solução

- 2.1.1.** A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
- 2.1.2.** O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
- 2.1.3.** A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
- 2.1.4.** Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
- 2.1.5.** Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução
- 2.1.6.** Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço
- 2.1.7.** Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.
- 2.1.8.** A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.2. Requisitos técnicos dos equipamentos que compõe a solução

- 2.2.1.** Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.2.2.** Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;
- 2.2.3.** Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;
- 2.2.4.** Deve Suportar, no mínimo, 6,5 (Seis virgula cinco) Gbps de throughput VPN IPSec;
- 2.2.5.** Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;
- 2.2.6.** Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;
- 2.2.7.** Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;
- 2.2.8.** Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
- 2.2.9.** Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.
- 2.2.10.** Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;
- 2.2.11.** Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;
- 2.2.12.** Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;
- 2.2.13.** Deve possuir porta console RJ-45;
- 2.2.14.** Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;
- 2.2.15.** Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
- 2.2.16.** Deve possuir Fontes redundantes.
- 2.2.17.** Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.
- 2.2.18.** Deve ser licenciado para uso pelo período de duração do contrato.
- 2.2.19.** Deve possuir garantia para uso pelo período de duração do contrato.

2.3. Firewalls de próxima geração (NGFW).

- 2.3.1.** A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gestão e monitoração.
- 2.3.2.** Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

- 2.3.3.** Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 2.3.4.** Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 2.3.5.** As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
- 2.3.6.** Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.
- 2.3.7. Funcionalidades de rede e firewall.**
- 2.3.8.** O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 2.3.9.** Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 2.3.10.** Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.3.11.** Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 2.3.12.** Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.3.13.** Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
- 2.3.14.** Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.3.15.** Deverá suportar sFlow ou Netflow;
- 2.3.16.** Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 2.3.17.** Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 2.3.18.** Deve suportar o protocolo padrão da indústria VXLAN;
- 2.3.19.** Deve implementar o protocolo ECMP;
- 2.3.20.** Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 2.3.21.** Enviar log para sistemas de monitoração externos;
- 2.3.22.** Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 2.3.23.** Deve possuir mecanismos de proteção anti-spoofing;
- 2.3.24.** Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 2.3.25.** Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.3.26.** Suportar OSPF graceful restart;
- 2.3.27.** Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.3.28.** Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 2.3.29.** Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 2.3.30.** Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 2.3.31.** A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 2.3.32.** Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 2.3.33.** O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 2.3.34.** A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 2.3.35.** A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 2.3.36.** Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 2.3.37.** Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 2.3.38.** Deverá suportar controle por zonas de segurança;
- 2.3.39.** Deverá suportar controles de políticas por porta e protocolo;
- 2.3.40.** Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 2.3.41.** Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 2.3.42.** Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 2.3.43.** Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
- 2.3.44.** Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 2.3.45.** Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- 2.3.46.** Suporte a objetos e regras IPV6;
- 2.3.47.** Suporte a objetos e regras multicast;
- 2.3.48.** Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos

automaticamente;

2.3.49. Funcionalidade de controle de aplicações.

2.3.50. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.3.51. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

2.3.52. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

2.3.53. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

2.3.54. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

2.3.55. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.3.56. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

2.3.57. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

2.3.58. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

2.3.59. Identificar o uso de táticas evasivas via comunicações criptografadas;

2.3.60. Atualizar a base de assinaturas de aplicações automaticamente;

2.3.61. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

2.3.62. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

2.3.63. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

2.3.64. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

2.3.65. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

2.3.66. Deve alertar o usuário quando uma aplicação for bloqueada;

2.3.67. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

2.3.68. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

2.3.69. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

2.3.70. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

2.3.71. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

2.3.72. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

2.3.73. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

2.3.74. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

2.3.75. Funcionalidade de prevenção de intrusão de ameaças.

2.3.76. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

2.3.77. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

2.3.78. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

2.3.79. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e "quarentenar" IP do atacante por um intervalo de tempo;

2.3.80. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

2.3.81. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.3.82. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

2.3.83. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.3.84. Deve permitir o bloqueio de vulnerabilidades;

- 2.3.85.** Deve permitir o bloqueio de exploits conhecidos;
- 2.3.86.** Deve incluir proteção contra ataques de negação de serviços;
- 2.3.87.** Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 2.3.88.** Detectar e bloquear a origem de portscans;
- 2.3.89.** Bloquear ataques efetuados por worms conhecidos;
- 2.3.90.** Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 2.3.91.** Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.3.92.** Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 2.3.93.** Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.3.94.** Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.3.95.** Identificar e bloquear comunicação com botnets;
- 2.3.96.** Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.3.97.** Os eventos devem identificar o país de onde partiu a ameaça;
- 2.3.98.** Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.3.99.** Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 2.3.100.** Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 2.3.101.** A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 2.3.102.** Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 2.3.103.** Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 2.3.104. Funcionalidade de filtro de conteúdo web e dns.**
- 2.3.105.** Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.3.106.** Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 2.3.107.** Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 2.3.108.** Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 2.3.109.** Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.3.110.** Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 2.3.111.** Possuir pelo menos 70 (setenta) categorias de URLs;
- 2.3.112.** Deve possuir a função de exclusão de URLs do bloqueio;
- 2.3.113.** Permitir a customização de página de bloqueio;
- 2.3.114.** Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 2.3.115.** Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 2.3.116.** Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 2.3.117.** Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;
- 2.3.118. Funcionalidade de identificação de usuários.**
- 2.3.119.** Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
- 2.3.120.** Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.3.121.** Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 2.3.122.** Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 2.3.123.** Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.3.124.** Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.3.125. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

2.3.126. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

2.3.127. Deve suportar o envio e recebimento de credenciais via RADIUS;

2.3.128. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

2.3.129. Funcionalidade de filtro de dados.

2.3.130. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

2.3.131. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

2.3.132. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

2.3.133. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.3.134. Funcionalidade de geolocalização.

2.3.135. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

2.3.136. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.3.137. Funcionalidade de vpn.

2.3.138. Suportar VPN Site-to-Site e Cliente-To-Site;

2.3.139. Suportar IPSec VPN;

2.3.140. A VPN IPSEC deve suportar 3DES;

2.3.141. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;

2.3.142. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

2.3.143. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

2.3.144. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

2.3.145. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI

2.3.146. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.3.147. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSEC IPv6;

2.3.148. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

2.3.149. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

2.3.150. Atribuição de DNS nos clientes remotos de VPN;

2.3.151. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

2.3.152. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

2.3.153. Suportar leitura e verificação de CRL (Certificate Revocation List);

2.3.154. Deverá manter uma conexão segura com o portal durante a sessão;

2.3.155. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

2.3.156. Funcionalidade de qos, traffic shaping e priorização de tráfego.

2.3.157. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

2.3.158. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

2.3.159. Endereço de origem e Endereço de destino;

2.3.160. Usuário e grupo;

2.3.161. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

2.3.162. Por porta;

2.3.163. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

2.3.164. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

2.3.165. O QoS deve possibilitar a definição de fila de prioridade;

2.3.166. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

2.3.167. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

2.3.168. Suportar modificação de valores DSCP para o Diffserv;

- 2.3.169.** Suportar priorização de tráfego usando informação de ToS (Type of Service);
- 2.3.170.** Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 2.3.171.** Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- 2.3.172.** Deve possibilitar a definição de bandas distintas para download e upload;
- 2.3.173. Funcionalidade de balanceamento inteligente de links.**
- 2.3.174.** A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 2.3.175.** A solução deve ser capaz de agregar vários links em uma interface virtual;
- 2.3.176.** A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 2.3.177.** A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 2.3.178.** A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 2.3.179.** A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 2.3.180.** A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
- 2.3.181.** A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 2.3.182.** Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 2.3.183.** Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
- 2.3.184.** Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 2.3.185.** Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 2.3.186.** A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 2.3.187.** A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 2.3.188.** A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 2.3.189.** Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 2.3.190.** A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;
- 2.3.191.** A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
- 2.3.192.** A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
- 2.3.193.** A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;
- 2.3.194.** A solução deve suportar nativamente conectores com clouds públicas;
- 2.3.195.** Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
- 2.3.196.** A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
- 2.3.197.** Deve implementar balanceamento de link por hash do IP de origem;
- 2.3.198.** Deve implementar balanceamento de link por hash do IP de origem e destino;
- 2.3.199.** Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 2.3.200.** O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;
- 2.3.201.** Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.
- 2.3.202. Funcionalidade de controlador de rede sem fio.**

- 2.3.203.** A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo;
- 2.3.204.** Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
- 2.3.205.** Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
- 2.3.206.** A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
- 2.3.207.** Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
- 2.3.208.** A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 2.3.209.** Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 2.3.210.** O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
- 2.3.211.** Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
- 2.3.212.** Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 2.3.213.** Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 2.3.214.** Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
- 2.3.215.** A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 2.3.216.** A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 2.3.217.** A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
- 2.3.218.** A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
- 2.3.219.** A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 2.3.220.** A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 2.3.221.** A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
- 2.3.222.** A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
- 2.3.223.** A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 2.3.224.** A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 2.3.225.** A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 2.3.226.** A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 2.3.227.** A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 2.3.228.** Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 2.3.229.** A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 2.3.230.** A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente

outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.3.231. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.3.232. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

2.3.233. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

2.3.234. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

2.3.235. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.3.236. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

2.3.237. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

2.3.238. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

2.3.239. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;

2.3.240. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.3.241. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

2.3.242. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

2.3.243. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

2.3.244. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

2.3.245. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

2.3.246. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

2.3.247. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

2.3.248. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

2.3.249. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

2.3.250. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

2.3.251. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

2.3.252. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.3.253. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

2.3.254. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.3.255. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

2.3.256. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

2.3.257. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

2.3.258. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

2.3.259. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

2.3.260. A solução deve permitir a configuração do captive portal com endereço IPv6;

2.3.261. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

2.3.262. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

2.3.263. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

2.3.264. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

2.3.265. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

- 2.3.266.** A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 2.3.267.** A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
- 2.3.268.** A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
- 2.3.269.** A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
- 2.3.270.** A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
- 2.3.271.** A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
- 2.3.272.** A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- 2.3.273.** A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
- 2.3.274.** A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
- 2.3.275.** A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
- 2.3.276.** A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
- 2.3.277.** A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
- 2.3.278.** A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
- 2.3.279.** A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
- 2.3.280.** A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
- 2.3.281.** A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- 2.3.282.** A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
- 2.3.283.** A solução deve possuir ferramentas de diagnósticos e debug;
- 2.3.284.** A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
- 2.3.285.** A solução deve suportar comunicação com elementos externos através de REST API;
- 2.3.286.** A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;
- 2.3.287. Funcionalidade de controlador de rede cabeada.**
- 2.3.288.** Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
- 2.3.289.** Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
- 2.3.290.** Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
- 2.3.291.** Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
- 2.3.292.** Deve montar a topologia da rede de maneira automática;
- 2.3.293.** Deve ser capaz de configurar os switches da rede;
- 2.3.294.** Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;
- 2.3.295.** Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 2.3.296.** Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 2.3.297.** Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 2.3.298.** Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 2.3.299.** Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 2.3.300.** Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard,;
- 2.3.301.** Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 2.3.302.** A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 2.3.303.** Deve ser capaz de configurar parâmetros SNMP dos switches;
- 2.3.304.** A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 2.3.305.** A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 2.3.306.** A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 2.3.307.** A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 2.3.308.** A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

- 2.3.309.** Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 2.3.310.** Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 2.3.311.** Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

2.4. Serviço de instalação firewall

2.4.1. Instalação Estrutura Física

- 2.4.2.** Levantamento de toda estrutura física do ambiente;
- 2.4.3.** Levantamento da estrutura Elétrica;
- 2.4.4.** Verificação do espaço a ser instalado os equipamentos;
- 2.4.5.** Abertura e conferência das caixas dos equipamentos;
- 2.4.6. Instalação do appliance físico:**
- 2.4.7.** Fixação do equipamento no RACK;
- 2.4.8.** Conexão da fonte de alimentação elétrica em régua de tomada;
- 2.4.9.** Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;
- 2.4.10.** Conexão das interfaces de rede com os switches;
- 2.4.11. Configuração do appliance físico:**
- 2.4.12.** Parametrização do Licenciamento;
- 2.4.13.** Parametrização das interfaces de rede;
- 2.4.14.** Atualização da última versão de Firmware;
- 2.4.15.** Parametrização das regras de NAT;
- 2.4.16.** Parametrização do Filtro de Conteúdo (WebFilter);
- 2.4.17.** Parametrização de Controle de Aplicação;
- 2.4.18.** Parametrização de VPN (Virtual Private Network);
- 2.4.19.** Parametrização IDS/IPS;
- 2.4.20.** Parametrização DNS;
- 2.4.21.** Parametrização de Gateway Antivírus;
- 2.4.22.** Parametrização de Objetos de Endereço;
- 2.4.23.** Parametrização de Grupo de Objetos;
- 2.4.24.** Parametrização de Load Balancing;
- 2.4.25.** Parametrização de SSO (Single Sign-on);
- 2.4.26.** Parametrização de SNMP;
- 2.4.27.** Parametrização de NTP;
- 2.4.28.** Parametrização de PortGroups;
- 2.4.29.** Parametrização de Zones;
- 2.4.30.** Parametrização de Serviços;
- 2.4.31.** Parametrização de Rotas;
- 2.4.32.** Parametrização de DHCP

2.5. Serviços profissionais de suporte técnico na solução de firewall

- 2.5.1.** Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;
- 2.5.2.** Efetuar toda rotina de backup das configurações semanalmente;
- 2.5.3.** Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;
- 2.5.4.** Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:
- 2.5.5.** Atividades relativas à Solução de Segurança:
- 2.5.6.** Criação das rotas para links.
- 2.5.7.** Criação de NAT.
- 2.5.8.** Liberação de portas.
- 2.5.9.** Configuração do Filtro de Conteúdo.
- 2.5.10.** Configuração do Controle de Aplicativos.
- 2.5.11.** Configuração do Agente para autenticação LDAP.
- 2.5.12.** Configuração para o Single Sign-On (SSO).
- 2.5.13.** Configurações dos serviços avançados de segurança (IPS, Antivírus).

2.5.14. Configuração de VPN client to site.

2.5.15. Configuração de VPN site to site.

2.5.16. Criação de regras de Firewall.

2.5.17. Criação de regras de QoS.

2.5.18. Emitir relatório de segurança mensal por localidade.

2.5.19. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.

2.5.20. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.

2.5.21. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

2.5.22. SLA dos serviços e atendimento

2.5.23. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

2.5.24. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

2.5.25. Gerar relatórios de acesso e desempenho da solução de firewall.

2.5.26. Deverá possuir sistema de abertura de chamados pela internet.

2.5.27. Monitorar latência e uptime dos links configurados.

2.5.28. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:

2.5.29. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.

2.5.30. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

2.5.31. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

2.5.32. Níveis de Severidade

2.5.33. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

2.5.34. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

2.5.34.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

2.5.34.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.5.35. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.5.35.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência

técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

2.5.35.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.5.36. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.5.36.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

2.5.36.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

2.5.37. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.5.37.1. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

2.5.37.2. Não poderá haver limites no quantitativo de abertura de chamados.

2.6. Qualificação Técnica

2.6.1. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

2.6.2. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

2.6.3. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

2.6.4. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas;

2.6.5. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan os trechos da documentação que comprovem os respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização.

3. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

3.1. Definição do objeto

3.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), serviços de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (Físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, serviços de rede, firewall (SonicWall), nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

3.1.2. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21 da Lei nº 14.133, de 2021.

3.1.3. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar.

3.1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

3.1.5. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

3.1.6. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

3.2. Características da solução

3.2.1. A execução do objeto seguirá a seguinte dinâmica:

3.2.2. Início da execução do objeto: 05 (cinco) dias úteis da emissão da ordem de serviço;

3.2.3. Descrição detalhada:

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12

02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

3.2.4. Contratada deve prestar os serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente.

3.2.5. A empresa deverá estar pronta para gerir toda a estrutura hiperconvergente, que conta atualmente com dois clusters gerenciados de forma separada (com armazenamento baseado em Software-defined storage -SDS), uma infraestrutura com base em acessos VDI, máquinas virtuais. A empresa contratada deve estar pronta para lidar com seus backups, restores, e qualquer problema, falha, atualização, instalação ou análise oriunda desta relação de ferramentas integradas.

3.3. Requisitos técnicos

3.3.1. Monitoramento e suporte técnico

3.3.2. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;

3.3.3. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:

3.3.4. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);

3.3.5. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;

3.3.6. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;

3.3.7. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

3.3.8. Manutenção, gestão de ativos e rede

3.3.9. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados no item 6.1.1, sem custo adicional;

3.3.10. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;

3.3.11. Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.

3.3.12. Executar a gestão técnica da infraestrutura de rede, abrangendo:

3.3.13. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;

3.3.14. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;

3.3.15. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;

3.3.16. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.

3.3.17. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

3.3.18. Serviços gerenciados

3.3.19. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;

3.3.20. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;

3.3.21. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;

3.3.22. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

3.3.23. Controle, inventário e chamados

3.3.24. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;

3.3.25. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

3.3.26. Logística e apoio à contratação

3.3.27. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;

3.3.28. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:

3.3.29. Elaboração de especificações técnicas;

3.3.30. Análise de propostas técnicas;

3.3.31. Apoio em processos licitatórios;

3.3.32. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

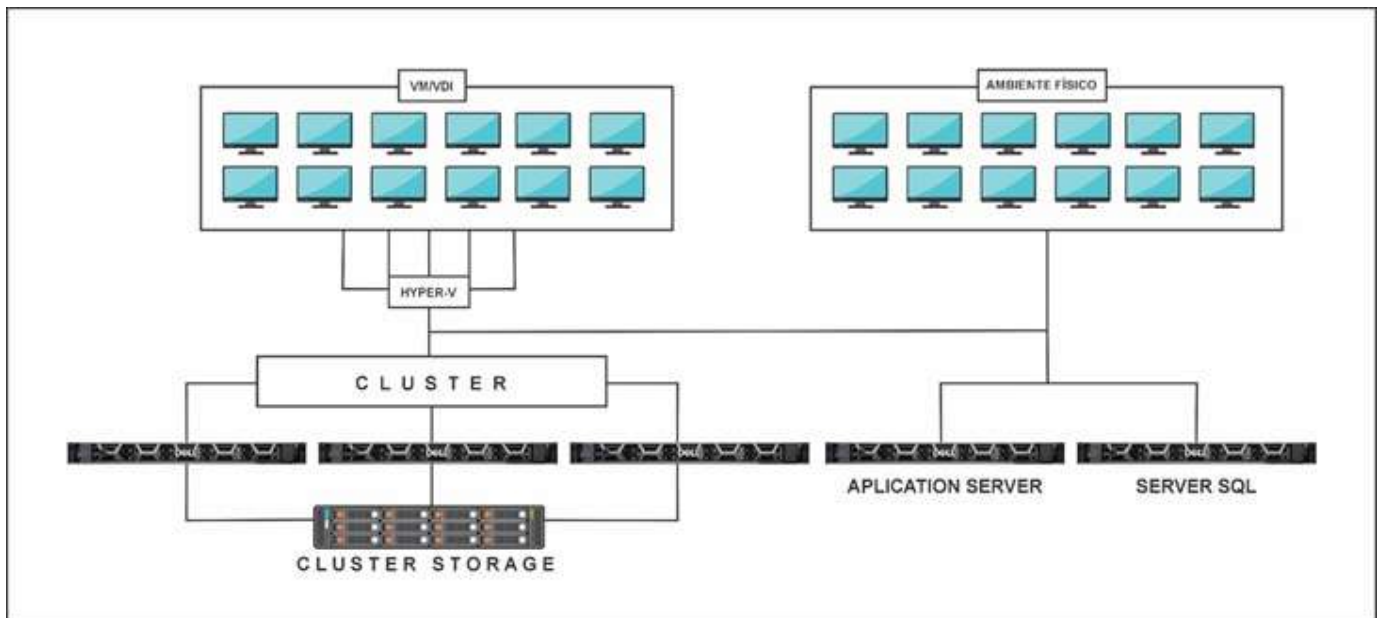
3.3.33. Atendimento presencial

3.3.34. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 8 (oito) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

3.3.35. Parque de informática do CRCES:

TIPO	DESCRIÇÃO	QUANTIDADE
Equipamento de segurança	Firewall a ser contratado neste termo de referência	01
Pontos de acesso	Pontos de acesso a serem contratados neste termo de referência	A depender da solução contratada
Virtualizador	Hyper-V	05
Servidor Windows 2022 Server	Dell PowerEdge R640	02
Servidor Windows 2022 Server	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01
Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01
Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados - VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01

3.3.36. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



1.1. **Manutenção preventiva e corretiva**

1.1.1. **Manutenção Preventiva**

1.1.2. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

1.1.3. Tais atividades incluem, mas não se limitam a:

1.1.4. Verificação de funcionamento dos componentes físicos e lógicos;

1.1.5. Limpeza técnica interna e externa;

1.1.6. Aferição e calibração de dispositivos, quando aplicável;

1.1.7. Atualização de firmwares, BIOS e softwares;

1.1.8. Verificação e otimização de configurações;

1.1.9. Avaliação do desempenho geral e análise de logs;

1.1.10. Testes de funcionalidade e conectividade.

1.1.11. Os equipamentos e ativos de tecnologia que deverão ser contemplados no plano de manutenção preventiva incluem:

1.1.12. Servidores físicos;

1.1.13. Servidores virtuais;

1.1.14. Infraestrutura de rede (switches, cabeamento, racks, patch panels, etc.);

1.1.15. Ativos de rede (roteadores, access points, controladoras, etc.);

1.1.16. Estações de trabalho tipo desktop;

1.1.17. Nobreaks e sistemas de energia ininterrupta;

1.1.18. Terminais de desktop virtualizado (Thin Clients);

1.1.19. Firewalls e appliances de segurança;

1.1.20. Notebooks;

1.1.21. Scanners (digitalizadores) de mesa e portáteis;

1.1.22. Projetores multimídia;

1.1.23. Monitores LCD/LED;

1.1.24. Telefones IP e demais dispositivos de comunicação;

1.1.25. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade e a descrição das atividades para cada tipo de equipamento e a metodologia empregada, a qual

manutenção preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.

1.1.26. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.

1.1.27. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.

1.1.28. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que solicitado.

1.1.29. Manutenção Corretiva

1.1.30. Em caso de surgimento de problema técnico em qualquer um dos equipamentos ou serviços listados no item de manutenção preventiva (item 6.1.3.1) a contratada deverá providenciar laudo técnico (item 5.1.7) e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.

1.1.31. CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.

1.1.32. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.

1.1.33. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.

1.1.34. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.

1.1.35. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 dias úteis após o recebimento dos novos equipamentos/peças.

1.1.36. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.

1.1.37. Durante a execução do serviço externo, a empresa contratada deverá:

1.1.38. Se responsabilizar pelo transporte dos equipamentos que serão retirados;

1.1.39. Providenciar termo de responsabilidade de retirada;

1.1.40. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

1.1.41. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;

1.1.42. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;

1.1.43. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;

1.1.44. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;

1.1.45. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto à qualidade do produto entregue;

1.1.46. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.

1.2. SLA dos serviços e atendimento

1.2.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

1.2.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

1.2.3. O ambiente de TI do CRCES deverá ser continuamente monitorado por ferramentas especializadas, com alertas automáticos e registro de falhas, a fim de garantir o funcionamento adequado e a disponibilidade dos recursos.

1.2.4. deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos

1.2.5. Deverá possuir sistema de abertura de chamados pela internet.

1.2.6. Monitorar latência e uptime dos links configurados.

1.2.7. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:

1.2.8. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.

1.2.9. Os níveis de atendimento técnico (N1, N2 e N3) deverão seguir o escopo descrito no item 1.3.3.3 a 1.3.3.6, com suporte remoto ilimitado e visitas técnicas presenciais duas vezes por semana, conforme cláusula 1.3.3.34.

1.2.10. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

1.2.11. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela , a seguir:

Níveis de Severidade

1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética (“cosméticos”), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

1.2.12. Níveis de Severidade

1.2.13. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

1.2.14. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

1.2.14.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

1.2.14.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

1.2.15. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

1.2.15.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

1.2.15.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

1.2.16. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

1.2.16.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

1.2.16.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

1.2.17. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

1.2.17.1. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

1.2.17.2. Não poderá haver limites no quantitativo de abertura de chamados.

1.3. Qualificação Técnica

1.3.1. A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se inviável:

1.3.2. Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.

1.3.3. Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.

1.3.4. Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.

1.3.5. Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.

1.3.6. Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.

1.3.7. Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o

funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.

1.3.8. Certificação ITIL v3 ou superior;

1.3.9. Certificação MCSA Windows Server 2012 ou superior;

1.3.10. A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:

1.3.11. Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;

1.3.12. Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;

1.3.13. Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

2. BACKUP CORPORATIVO

2.1. Software de Backup

2.1.1. Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,

2.1.2. Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.

2.1.3. Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.

2.1.4. Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.

2.1.5. Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.

2.1.6. Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.

2.1.7. Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.

2.1.8. Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.

2.1.9. Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.

2.1.10. Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.

2.1.11. Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.

2.1.12. Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.

2.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações: O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.

2.1.14. Backup Incremental e Diferencial: Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.

2.1.15. Cópias de Backup Imutáveis: Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.

2.1.16. Retenção Personalizável: O software deve oferecer flexibilidade na configuração de políticas de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.

2.1.17. Arquivamento Inteligente: Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.

2.1.18. Monitoramento e Alertas: O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.

2.1.19. Dashboard Intuitivo: Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.

2.1.20. Otimização de Recursos (IOPS e Throughput): O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.

2.1.21. Restauração Granular: Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.

2.1.22. Recuperação Bare-Metal: Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.

2.1.23. Testes de Restauração Automática: Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.

2.1.24. Integração Nativa com Provedores de Nuvem: Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.

2.1.25. Economia de Largura de Banda: Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.

2.1.26. Perfis de Acesso Personalizáveis: O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que

apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.

2.1.27. Controle de Acessos Granular: Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.

2.1.28. Suporte a LGPD e Outras Normas: O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.

2.1.29. Auditorias e Relatórios: Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.

2.1.30. Automatização de trabalhos de Backup: Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.

2.1.31. Integração com Ferramentas de Orquestração: Suporte para integração com ferramentas de orquestração e automação (ex: scripts PowerShell, APIs).

2.1.32. Cobertura Completa: O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.

2.1.33. Recuperação Granular: Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.

2.1.34. Agendamento e Automação: A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

2.2. Appliance de Backup Local

2.2.1. A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.

2.2.2. Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.

2.2.3. Será responsável por configurar o sistema de armazenamento local do equipamento, devendo:

2.2.3.1. Criar e configurar o arranjo de discos em RAID 5;

2.2.3.2. Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);

2.2.3.3. Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas

2.2.4. Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.

2.2.5. Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:

2.2.5.1. Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;

2.2.5.2. Gerar e manter registros e relatórios de status dos backups locais e remotos;

2.2.5.3. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

2.2.6. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:

2.2.6.1. Acompanhamento da integridade dos discos e volumes lógicos;

2.2.6.2. Monitoramento do uso de espaço em disco e alertas proativos;

2.2.6.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

2.2.7. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:

2.2.7.1. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;

2.2.7.2. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).

2.2.8. deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:

2.2.8.1. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;

2.2.8.2. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;

2.2.8.3. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;

2.2.8.4. Ajustar as políticas de backup e monitoramento para o novo ambiente.

2.2.9. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

2.3. Armazenamento de backup em nuvem

2.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.

2.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.

2.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.

2.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

- 2.3.5.** O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.
- 2.3.6.** A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.
- 2.3.7.** A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.
- 2.3.8.** Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.
- 2.3.9.** O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
- 2.3.10.** O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).
- 2.3.11.** TLS/SSL deve ser usado para proteger os dados durante a transferência.
- 2.3.12.** Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.
- 2.3.13.** Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.
- 2.3.14.** O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.
- 2.3.15.** O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.
- 2.3.16.** Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.
- 2.3.17.** A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.
- 2.3.18.** O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.
- 2.3.19.** Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.
- 2.3.20.** Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).
- 2.3.21.** O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.
- 2.3.22.** A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e possíveis falhas.
- 2.3.23.** Ferramentas de monitoramento nativas devem estar integradas.
- 2.3.24.** Os custos devem estar inclusos na cobrança mensal do armazenamento.

2.4. SLA dos serviços e atendimento

- 2.4.1.** Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 2.4.2.** Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 2.4.3.** deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime e falhas críticas.
- 2.4.4.** Deverá possuir sistema de abertura de chamados pela internet.
- 2.4.5.** A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 2.4.6.** O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 2.4.7.** Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 2.4.8.** Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela , a seguir:

Níveis de Severidade	
1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.
3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup..
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

2.4.9. Níveis de Severidade

- 2.4.10.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

2.4.11. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

2.4.11.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

2.4.11.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.4.12. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.4.12.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

2.4.12.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.4.13. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.4.13.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

2.4.13.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

2.4.14. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.4.14.1. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

2.4.14.2. Não poderá haver limites no quantitativo de abertura de chamados.

2.3.3.17. Certificações

Será necessário solicitar algumas certificações, com isso o CRCES está garantindo que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade, alinhado com as melhores práticas do mercado e com as recomendações de segurança de órgãos como o NIST e o CIS.

Abaixo, vamos citar cada uma delas, ampliando as justificativas:

a) Certificação Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 (no mínimo)

Domínio do Sistema Operacional: A certificação MCSA garante que o profissional possui um conhecimento profundo do Windows Server 2012, que é a base do nosso ambiente corporativo hiperconvergente. Isso inclui domínio em instalação, configuração, administração e troubleshooting do sistema operacional, além de serviços como Active Directory, DNS, DHCP e outros.

Integração com Outros Serviços: O Windows Server é integrado a outros serviços da Microsoft, como Exchange, SharePoint e SQL Server. Um profissional com a certificação MCSA terá mais facilidade em integrar e gerenciar esses serviços em um ambiente unificado.

Padrão de Qualidade e Alinhamento com Boas Práticas: A certificação MCSA é reconhecida mundialmente como um padrão de qualidade para profissionais de infraestrutura. Ela demonstra que o profissional possui as habilidades necessárias para lidar com as complexidades de um ambiente como o nosso, que possui dois clusters e funciona no modelo de hiperconvergência, além de estar alinhado com as melhores práticas do mercado.

b) Certificação para Instalação e Configuração de Switches DELL ou similar

Infraestrutura de Rede e Otimização: Switches são equipamentos essenciais para a interconexão de dispositivos em uma rede. A certificação garante que o profissional possui conhecimento sobre os princípios de funcionamento de switches, além de saber como configurá-los para atender às necessidades específicas da rede do CRCES, que utiliza switches complexos de alta tecnologia (tanto o core quanto o de agregação da hiperconvergência) Isso permite otimizar o desempenho da rede, reduzindo a latência e aumentando a disponibilidade.

Escalabilidade e Flexibilidade: À medida que a rede cresce, é necessário adicionar novos switches. Um profissional certificado terá as habilidades necessárias para integrar novos switches à rede existente, garantindo a escalabilidade da infraestrutura e a flexibilidade para atender às futuras demandas do CRCES.

Alinhamento com as Melhores Práticas: A certificação garante que o profissional está familiarizado com as melhores práticas de configuração e gerenciamento de redes, o que contribui para a estabilidade e a segurança da infraestrutura.

As certificações solicitadas demonstram que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade para o CRCES. Elas garantem que os profissionais terão a capacidade de:

Gerenciar e manter a infraestrutura de TI de forma eficiente, segura e alinhada com as melhores práticas do mercado.

Resolver problemas de forma rápida e eficaz, minimizando o tempo de inatividade do sistema.

Implementar novas tecnologias de forma adequada e segura.

Acompanhar as melhores práticas do mercado e as recomendações de segurança de órgãos como o NIST e o CIS.

2.3.3.17.1. Justificativa

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada para gerar todos esses serviços de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da

gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a) **Assegurar a contratação da empresa mais qualificada e experiente para o serviço.**
- b) **Definir claramente as expectativas e responsabilidades de ambas as partes.**
- c) **Permitir a avaliação objetiva das propostas e a escolha da melhor solução.**
- d) **Facilitar o acompanhamento e a fiscalização do contrato.**
- e) **Mitigar riscos e garantir o sucesso da contratação.**
- f) **Atender aos princípios da Lei 14.133 e da Administração Pública.**

Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:

- a) **Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.**
- b) **Aumento de custos com retrabalho, correções e possíveis perdas.**
- c) **Dificuldades na comunicação e na resolução de conflitos.**
- d) **Dificuldades na fiscalização do contrato e na cobrança de resultados.**
- e) **Riscos de inadimplência e de litígios.**

A contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.

2.3.3.18. Softwares que deverão ser disponibilizados

As ferramentas listadas abaixo (monitoramento e de abertura de chamados) deverão ser disponibilizadas e totalmente configuradas pela CONTRATADA sem custo adicional para o CRCES, e deverão apresentar as seguintes especificações (mínimas):

2.3.3.18.1. Ferramenta de monitoramento.

Monitoramento de Rede: Roteadores, switches, impressoras, etc., utilizando protocolos como SNMP (v1/v2c/v3), ICMP (ping) e verificações de portas TCP/UDP.

Monitoramento de Servidores: Desempenho de CPU, uso de memória, espaço em disco, tráfego de rede, processos, serviços e logs.

Monitoramento de Aplicações e Serviços: Bancos de dados (MySQL, PostgreSQL, Oracle, etc.), servidores web (Apache, Nginx, IIS), Java applications (JMX), serviços específicos e outros.

Monitoramento de Virtualização: Serviços em nuvem, contêineres, máquinas virtuais.

Monitoramento Web (Web Scenarios): Simula a navegação de usuários em aplicações web, verificando a disponibilidade, o tempo de resposta e o conteúdo das páginas.

Monitoramento de Dispositivos IoT e Sensores: Coleta dados de uma variedade de sensores e dispositivos IoT.

Monitoramento de Logs e Eventos: Analisa arquivos de log em busca de padrões, erros, avisos ou atividades suspeitas.

Extensibilidade: Permitir a coleta de dados qualquer fonte através de scripts externos personalizados, APIs e extensões.

Limiares Flexíveis: Definição de condições personalizadas para identificar problemas (triggers).

Previsão de Tendências e Machine Learning: Funções preditivas que permitem prever quando um limiar será atingido, possibilitando ações proativas antes que um problema ocorra.

Níveis de Severidade: Classificação dos problemas por níveis de severidade (informação, aviso, médio, alto, desastre), facilitando a priorização.

Análise de Causa Raiz: Ajuda a identificar a causa subjacente dos problemas.

Canais de Notificação Diversos: Envio de alertas por e-mail, SMS, aplicativos de mensagens (Telegram, Slack, etc.), webhooks e scripts personalizados.

Escalonamento de Alertas: Configuração de fluxos de escalonamento para garantir que os alertas cheguem aos destinatários corretos em diferentes etapas.

Ações Automáticas (Auto-remediação): Possibilidade de executar comandos remotos automaticamente em resposta a um problema (ex: reiniciar um serviço, executar um script de correção).

Notificações Customizáveis: Mensagens de alerta personalizadas com informações relevantes sobre o problema.

Dashboards Personalizáveis: Criação de painéis de controle interativos com widgets para exibir métricas em tempo real, status de hosts, problemas, mapas de rede, gráficos e muito mais.

Gráficos Flexíveis: Geração de gráficos detalhados para visualizar dados históricos e tendências, com opções de personalização de tempo e exibição.

Mapas de Rede (Network Maps): Criação de representações visuais da infraestrutura, mostrando o status dos dispositivos e as interconexões.

Relatórios: Geração de relatórios de disponibilidade, desempenho e outros dados relevantes.

Visão de Negócio (SLA/KPI): Possibilidade de monitorar o desempenho dos serviços de TI em relação aos Acordos de Nível de Serviço (SLAs) e Indicadores Chave de Desempenho (KPIs).

Descoberta Automática de Rede (Network Discovery): Detecta automaticamente novos dispositivos na rede, facilitando a configuração inicial.

Auto-registro de Agentes (Agent Autoregistration): Permite que os agentes Zabbix se registrem automaticamente no servidor Zabbix, simplificando a implantação em grande escala.

Descoberta de Baixo Nível (Low-Level Discovery - LLD): Descobre automaticamente componentes de um host (ex: interfaces de rede, sistemas de arquivos, CPUs, partições de disco) e cria itens de monitoramento, triggers e gráficos para eles.

Modelos (Templates): Reutilização de configurações de monitoramento para diferentes tipos de hosts, agilizando a implantação e padronizando o monitoramento.

Sistema de Permissões: Controle granular de acesso baseado em funções e grupos de usuários.

Autenticação: Suporte a diferentes métodos de autenticação (interna, LDAP, SAML).

criptografia: Criptografia de todo o tráfego de monitoramento para garantir a segurança dos dados.

Alta Disponibilidade: Monitoramento contínuo.

2.3.3.18.2. Ferramenta de abertura e gestão de chamados de T.I

Abertura de chamados por e-mail: Integração com e-mail para que os chamados sejam criados automaticamente a partir de mensagens enviadas para um endereço específico.

Categorização e Priorização Automática: Possibilidade de pré-definir categorias (ex: "Problema de Software", "Solicitação de Hardware", "Acesso"), subcategorias e níveis de prioridade (ex: "Baixa", "Média", "Alta", "Crítica") com base no tipo de solicitação ou no usuário.

Anexos: Capacidade de anexar arquivos (screenshots, logs, documentos) para fornecer mais contexto ao chamado.

Atribuição Automática e Manual: Atribuição de chamados a agentes ou equipes com base em regras predefinidas (categoria, prioridade, departamento do usuário) ou atribuição manual pelos gerentes.

Filas de Atendimento: Organização dos chamados em filas específicas para cada equipe ou tipo de serviço.

Fluxos de Trabalho (Workflows): Definição de etapas e ações automatizadas para o ciclo de vida de um chamado (ex: Aberto -> Em Andamento -> Aguardando Usuário -> Resolvido -> Fechado).

Notificações Automáticas: Envio de e-mails ou notificações push para o usuário e para os agentes sobre o status do chamado, novas mensagens, resolução, etc.

Colaboração em Equipe: Permite que múltiplos agentes trabalhem em um mesmo chamado, com compartilhamento de informações e anotações.

Macros/Respostas Predefinidas: Modelos de respostas para perguntas frequentes, agilizando o atendimento.

Artigos e FAQs: Repositório central de artigos de solução de problemas, FAQs (perguntas frequentes), guias e procedimentos.

Busca Inteligente: Ferramenta de busca robusta que permite aos usuários e agentes encontrar informações relevantes rapidamente.

Sugestão de Soluções: Apresentar artigos da base de conhecimento aos usuários enquanto eles digitam seu problema no portal self-service, incentivando a auto-resolução.

Dashboards e Métricas: Visualização em tempo real de KPIs (Key Performance Indicators) como número de chamados abertos, chamados resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

Relatórios Customizáveis: Geração de relatórios sobre desempenho da equipe, tipos de chamados mais comuns, cumprimento de SLAs, tendências, etc.

Integração com a ferramenta de Monitoramento: Integração com a ferramenta de monitoramento proposto pela CONTRATADA, para que alertas de monitoramento possam gerar chamados automaticamente.

Controle de Acesso Baseado em Funções: Definição de permissões diferentes para usuários, agentes e administradores.

Acessibilidade: Interface amigável e acessível em diferentes dispositivos (desktop, mobile).

SLA (Service Level Agreement) Management:

Definição de SLAs para diferentes tipos de chamados, especificando tempo de resposta e tempo de resolução esperados.

Monitoramento automático do cumprimento dos SLAs, com alertas e escalonamentos caso os prazos estejam sendo excedidos.

Escalonamento automático para gerentes ou equipes superiores quando os SLAs estão em risco.

Histórico Completo do Chamado: Registro detalhado de todas as interações, atualizações, comentários e mudanças de status em um chamado.

Pesquisa Avançada: Facilidade para buscar chamados por ID, usuário, categoria, palavras-chave, etc.

2.3.3.19. Serviços externos que deverão ser acompanhados pela contratada

A CONTRATADA será um ponto focal e estratégico para o CRCES, atuando como o principal **elo de coordenação e intermediação** entre nossa instituição e as demais prestadoras de serviços de TI. Dada a complexidade e a interdependência de nossas operações tecnológicas, a **intervenção e o acompanhamento proativo** da CONTRATADA serão cruciais para garantir a fluidez e a eficácia de todas as interações e projetos. Atualmente, gerenciamos diversos contratos com terceiros, e essa carteira de fornecedores poderá se expandir conforme nossas necessidades evoluírem. Abaixo vamos listar alguns dos contratos:

- Serviço de fornecimento de software de gestão integrada (SpiderWare);
- Serviço de hospedagem do website e webservice do CRCES;
- Serviço de fornecimento de link de internet;
- Serviço de fornecimento de e-mail corporativo;
- Serviço de fornecimento de link SIP Trunk;
- Serviço de fornecimento de validador de assinaturas digitais;
- Serviço de fornecimento de atendente virtual por whatsapp;
- Serviço de outsourcing de impressão;

· Serviço de fornecimento de ePABX;

2.4 - ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE DÃO SUPORTE;

2.4.1 A estimativa de quantidade foi baseada na estrutura de tecnologia atual do CRCES, conforme descrito ao longo deste documento.

2.5 - LEVANTAMENTO DE MERCADO, ANÁLISE DAS ALTERNATIVAS POSSÍVEIS E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO SOLUÇÃO A CONTRATAR;

2.5.1 O levantamento de mercado para contratação de empresa que preste serviço de gerenciamento de T.I e um processo que requer atenção, cuidado e critério, pois envolve a confiança e a parceria entre o contratante e o contratado.

2.5.2 Atualmente, o CRCES enfrenta um cenário desafiador na gestão de T.I, com apenas um funcionário dedicado a essa área. Esta escassez representa um risco significativo para a continuidade dos serviços e para a qualidade do atendimento oferecido aos usuários.

2.5.3 Ademais, o CRCES se depara com desafios crescentes, como a necessidade premente de adaptação às normas de governança, a demanda por inovação e modernização tecnológica, bem como a crescente complexidade dos processos e projetos de T.I.

2.5.4 Em um ambiente em constante evolução tecnológica, é essencial que o CRCES esteja alinhado com as mais recentes tendências e práticas em T.I. A falta de recursos e expertise interna dificulta a implementação de soluções inovadoras que possam impulsionar a eficiência e a eficácia das operações.

2.5.5 O serviço de gerenciamento de T.I são considerados serviços comuns, pois se enquadram na definição de atividades que podem ser prestadas por qualquer pessoa jurídica, sem exigência de qualificação específica ou exclusividade.

2.5.6 Uma vez que há diversas empresas que oferecem este serviço, optamos por consultar empresas que já têm experiência com a infraestrutura tecnológica do CRCES, o que nos permite obter uma pesquisa mais adequada à realidade e à necessidade do suporte e serviço que solicitamos no processo, com isso, alcançamos a estimativa descrita abaixo:

	VALOR ITEM I
Mensal	R\$
Anual	R\$

2.5.7 Analisando os orçamentos apresentados, o valor mensal para esta contratação ficou estimado em R\$ xxx), sendo que o valor total para os 12 (doze) meses resulta no valor de R\$ xxxx para os serviços gerenciados em Tecnologia da Informação.

2.5.10 Além disso, o Conselho Regional de Contabilidade do Espírito Santo, como órgão público, tem a responsabilidade de zelar pelo uso eficiente dos recursos financeiros. Portanto, a busca pelo menor preço em processos de contratação é uma prática comum para garantir a economicidade e maximizar o retorno sobre o investimento público.

2.5.11 Outro aspecto relevante é a transparência e a simplificação do processo de licitação proporcionadas pelo critério de "menor preço". Por ser um critério objetivo de verificação, ele facilita a análise das propostas pelos licitantes e pelos responsáveis pela fiscalização, promovendo assim a lisura e a competitividade do certame.

2.5.12 Por fim, considerando que os **Serviços gerenciados em Tecnologia da Informação** são essenciais para garantir a saúde e a segurança dos ocupantes das instalações do Conselho Regional de Contabilidade, a escolha do critério de "menor preço" permite contar com uma infraestrutura de tecnologia da informação (T.I) eficiente, segura e atualizada, que garanta o bom funcionamento dos sistemas internos e externos, a comunicação com os diversos públicos e a proteção dos dados sensíveis.

2.5.13 Dessa forma, o uso do critério de "menor preço" no processo de licitação para a contratação de serviços **Tecnologia da Informação** completa é uma escolha justificada e alinhada aos princípios da administração pública, visando garantir a eficiência, a transparência e o melhor aproveitamento dos recursos disponíveis.

2.6 - ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Conforme documentos acostados aos autos, o valor estimado da contratação mensal é de R\$40.000,00 (quarenta mil reais) perfazendo o valor total de R\$480.000,00 (quatrocentos e oitenta mil reais).

Para fins de estimativa da presente contratação, procedeu-se à pesquisa direta com fornecedores, por meio de solicitação de proposta de preço por e-mail, cujo valor médio é apresentado acima.

A pesquisa está em conformidade com o art. 6º da Instrução Normativa SEGES/ME n.º 65/2021, realizamos a média dos orçamentos.

2.7 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, INCLUSIVE DAS EXIGÊNCIAS RELACIONADAS À MANUTENÇÃO E À ASSISTÊNCIA TÉCNICA QUANDO FOR O CASO;

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

Na descrição da solução, já estão incluídos todos os procedimentos, equipamentos, instalação e manutenções corretivas para a perfeita execução

aos serviços.

2.8 - JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO;

A não viabilidade de parcelamento da solução se fundamenta na natureza integrada do objeto, que demanda uma abordagem unificada para garantir eficiência e consistência. Optar por consolidar os serviços em um único item considerou a coesão dos elementos a serem licitados e a sequência lógica de sua execução.

Adicionalmente, a fragmentação deste processo acarretaria à Administração um risco significativo, pois diferentes empresas, embora possam operar no mesmo setor, apresentam disparidades estruturais, logísticas e econômico-financeiras. Tal divisão resultaria em capacidades discrepantes de prestação de serviço, comprometendo a supervisão e expondo a execução dos contratos a possíveis desvios dos padrões estabelecidos.

Portanto, a decisão de não parcelar a contratação busca assegurar a coerência e a qualidade na entrega dos serviços, minimizando potenciais incongruências e garantindo a conformidade na execução do objeto.

2.9 - RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS;

Pretende-se com a presente contratação, os resultados abaixo descritos:

- Aumentar a eficiência e a segurança dos sistemas de informação do CRCES, reduzindo os riscos de falhas, perdas ou vazamentos de dados.
- Garantir a continuidade das atividades do CRCES em caso de eventuais problemas técnicos, desastres naturais ou ataques cibernéticos, por meio de um plano de recuperação de desastres baseado em backup em nuvem.
- Otimizar os custos e os recursos do CRCES, evitando gastos desnecessários com infraestrutura, manutenção e atualização de equipamentos e softwares.
- Melhorar o atendimento e a satisfação dos profissionais da contabilidade e da sociedade em geral, oferecendo serviços de qualidade, rapidez e confiabilidade.

2.10 - PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Para a execução do objeto deste estudo, não há necessidade de nenhuma adequação do ambiente do órgão.

2.11 - CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES;

Para o objeto deste estudo, não são necessárias contratações correlatas ou interdependentes.

2.12 - DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, QUANDO APLICÁVEL;

Não se aplica a esta contratação.

2.13 - POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA.

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada em gerenciamento de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a. Assegurar a contratação da empresa mais qualificada e experiente para o serviço.
- b. Definir claramente as expectativas e responsabilidades de ambas as partes.
- c. Permitir a avaliação objetiva das propostas e a escolha da melhor solução.
- d. Facilitar o acompanhamento e a fiscalização do contrato.
- e. Mitigar riscos e garantir o sucesso da contratação.
- f. Atender aos princípios da Lei 14.133 e da Administração Pública.
- g. Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:
- h. Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.
- i. Aumento de custos com retrabalho, correções e possíveis perdas.
- j. Dificuldades na comunicação e na resolução de conflitos.
- k. Dificuldades na fiscalização do contrato e na cobrança de resultados.
- l. Riscos de inadimplência e de litígios.
- m. Em suma, a contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.
- n. Investir em um Termo de Referência bem elaborado é um investimento na segurança, confiabilidade e no sucesso da gestão da TI do CRCES.
- o. Além disso, essa medida promove transparência e integridade, uma vez que impede o envolvimento de terceiras partes que possam diluir a responsabilidade direta da contratada. A restrição à exploração industrial visa, ainda, assegurar que o objeto seja destinado exclusivamente ao cumprimento das finalidades públicas, sem desvios para utilização comercial ou industrial que contrariem o interesse público.

p. Para comprovação de capacidade, deve exigir-se que os licitantes apresentem atestados técnicos que demonstrem a execução dos serviços com infraestrutura própria e sem uso de exploração industrial, atendendo assim ao critério de "estrutura própria" e garantindo os altos padrões esperados.

Com base nas informações estabelecidas neste documento, nas justificativas apresentadas no Documento de Formalização da Demanda – DFD, a Equipe de Planejamento DECLARA a viabilidade da contratação de empresa especializada, Serviços de TI inclui a gestão de redes, ativos de rede, servidores, estações de trabalho, nobreaks e monitores. A empresa será responsável por suporte técnico remoto e presencial, manutenção preventiva e corretiva, e monitoramento de links de internet e infraestrutura hiperconvergente.

3. Normativos que disciplinam o serviço a ser contratado:

[Lei nº 14.133](#), de 1º de abril de 2021 - Lei de Licitações e Contratos Administrativos.

[Decreto nº 10.947](#), de 25 de janeiro de 2022 - Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

[Decreto nº 7.174](#), de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

[Instrução Normativa SGD/MGI nº 6](#) de 29 de março de 2023 - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

[Instrução Normativa SGD/ME nº 94](#) de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

[Instrução Normativa SLTI nº 01](#), de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

4. Do Acesso às Informações contidas nos presentes Estudos Preliminares:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que:

☒	As informações contidas nos presentes Estudos Preliminares DEVERÃO ESTAR DISPONÍVEIS para qualquer interessado, pois não se caracterizam como sigilosas.
☐	As informações contidas nos presentes Estudos Preliminares ASSUMEM CARÁTER SIGILOSO . Nos termos do Art. 23 da Lei nº 12.527/2011, e, portanto, deverão ter acesso restrito.

5. Equipe de Planejamento:

São responsáveis pela elaboração do presente documento que materializa os Estudos Preliminares da presente contratação os seguintes servidores:

Wekson José Barbieri Mariano Matrícula 87 Membro da Equipe de Planejamento	Elaine Leopoldino Ferreira Matrícula 198 Membro da Equipe de Planejamento	Rodrigo dos Santos Sanz Matrícula 50 Membro da Equipe de Planejamento



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 22/08/2025, às 07:49, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 22/08/2025, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 16/09/2025, às 10:41, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0930157** e o código CRC **0E0F01CA**.



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

ANÁLISE DE RISCOS

Processo nº 9079618110000798.000048/2025-57

RISCOS DO PROCESSO DE CONTRATAÇÃO

Risco 1

Risco: Indisponibilidade de serviços críticos (rede, firewall, backup).

Probabilidade: Média.

Dano: Paralisação de atividades administrativas, perda de produtividade.

Impacto: Alto.

Id	Ação Preventiva	Responsável
1	Definir SLA com prazos rígidos para atendimento remoto e presencial.	Contratado + Fiscal do Contrato
2	Monitoramento e relatórios periódicos de desempenho.	Contratado

Id	Ação de Contingência	Responsável
1	Acionamento imediato do suporte presencial em falhas críticas.	Contratado
2	Utilizar plano de contingência de internet/backup alternativo.	CRCES + Contratado

Risco 2

Risco: Falhas na gestão e manutenção do banco de dados SQL Server.

Probabilidade: Baixa.

Dano: Perda ou inconsistência de dados estratégicos.

Impacto: Alto.

Id	Ação Preventiva	Responsável
1	Manutenção preventiva periódica no banco de dados.	Contratado
2	Implementação de rotinas de backup testadas regularmente.	Contratado

Id	Ação de Contingência	Responsável

Id	Ação de Contingência	Responsável
1	Restaurar banco a partir do backup mais recente.	Contratado
2	Escalonar incidente para equipe especializada de banco de dados.	Contratado

RISCOS RELACIONADOS AO FORNECEDOR

Risco 1

Risco: Fornecedor sem capacidade técnica ou equipe qualificada.

Probabilidade: Média.

Dano: Execução inadequada dos serviços, falhas recorrentes.

Impacto: Alto.

Id	Ação Preventiva	Responsável
1	Exigir certificações e atestados de capacidade técnica.	Comissão de Licitação
2	Avaliar portfólio de contratos similares.	Área Técnica/Fiscal

Id	Ação de Contingência	Responsável
1	Notificação e aplicação de penalidades contratuais.	CRCES
2	Acionar contrato emergencial ou backup com outro fornecedor.	CRCES

Risco 2

Risco: Risco de continuidade (problemas financeiros ou estruturais do fornecedor).

Probabilidade: Baixa.

Dano: Interrupção do contrato antes do prazo.

Impacto: Médio.

Id	Ação Preventiva	Responsável
1	Exigir certidões fiscais, trabalhistas e análise de balanço.	Comissão de Licitação
2	Prever cláusulas contratuais para rescisão e substituição.	Jurídico

Id	Ação de Contingência	Responsável
1	Substituição imediata do fornecedor por nova licitação/contrato emergencial.	CRCES
2	Manter equipe de TI interna de apoio em caso de transição.	CRCES



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 22/08/2025, às 08:53, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 22/08/2025, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 16/09/2025, às 11:33, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0952056** e o código CRC **D5CD5964**.



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

NLL - TERMO DE REFERENCIA DE TIC

Processo nº 9079618110000798.000048/2025-57

1. DEFINIÇÃO DO OBJETO

1.1. Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O prazo de vigência da contratação é de 12 (doze) meses contados dos da assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.3.1. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar;

1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual .

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares

4. REQUISITOS DA CONTRATAÇÃO

4.1. Sustentabilidade

4.1.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.1.2. Garantia da contratação

4.1.2.1. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#), tendo em vista que o pagamento pelos serviços somente será realizado após a referida prestação e atesto pelo fiscal de contrato. Além disso, em caso de problema que se apresente posteriormente, o CRCES poderá instaurar procedimento administrativo sancionador com base na legislação vigente.

4.1.3. Vistoria

4.1.3.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo e-mail: administrativo@crc-es.org.br.

4.1.3.1.1. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

4.1.3.2. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.1.3.3. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.1.3.4. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.1.4. Local e horário da prestação dos serviços

4.1.5. Os serviços serão prestados na sede do CRCES, localizada na Rua Amélia da Cunha Ornelas, nº 30, Bairro Bento Ferreira, Vitória/ES – CEP: 29.050-620 Rotinas a serem cumpridas.

4.1.6. Materiais a serem disponibilizados

4.1.7. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

4.1.8. Informações relevantes para o dimensionamento da proposta

4.1.9. A Contratada deverá prestar serviços gerenciados de Tecnologia da Informação que abrangem o suporte técnico avançado (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a gestão de incidentes e mudanças. O escopo prevê a gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), com o fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, e a gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais. Será responsável também pelo monitoramento contínuo da infraestrutura, com identificação e mitigação proativa de riscos, pela manutenção preventiva e corretiva de todo o parque de TI, pela gestão e monitoramento dos links de internet, pela gestão e manutenção da infraestrutura hiperconvergente e do banco de dados em SQL Server. Além disso, inclui o fornecimento, instalação e gestão de um Firewall de Próxima Geração e a implementação e gestão de solução de backup local e em nuvem. Os serviços atenderão a única localidade do CRCES, até 60 estações de trabalho (físicas ou virtuais), 5 servidores físicos e 12 servidores virtuais.

4.1.10. A empresa contratada deverá estar plenamente capacitada para gerenciar toda a estrutura de TI híbrida do CRCES. Esta estrutura é complexa e inclui uma infraestrutura hiperconvergente (com armazenamento baseado em Software-defined Storage - SDS), uma infraestrutura com acessos VDI (Virtual Desktop Infrastructure), máquinas virtuais e uma infraestrutura tradicional (com desktops

físicos e notebooks). A Contratada será responsável por assegurar a gestão completa dos backups e restores de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a disponibilidade e integridade dos dados em todas as plataformas.

4.1.11. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

4.1.12. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

4.1.13. Procedimentos de transição e finalização do contrato

4.1.14. Apresentar relatório final de atividades, contendo o resumo dos serviços executados, as ocorrências técnicas registradas, pendências identificadas e orientações para continuidade da operação da infraestrutura de TI, incluindo rede, segurança da informação, backup e suporte.

4.1.15. Entregar toda a documentação técnica e operacional produzida durante a execução do contrato, em meio físico e/ou digital, de forma organizada, classificada e atualizada, contemplando registros de configuração de equipamentos, scripts, inventários, diagramas de rede, manuais operacionais e demais documentos que garantam a rastreabilidade e integridade das informações

4.1.16. Transferir conhecimentos e informações relevantes ao(s) servidor(es) designado(s) pela Administração, por meio de reuniões técnicas, relatórios explicativos e capacitação operacional, com foco nos processos relacionados à infraestrutura de redes, segurança da informação, monitoramento e procedimentos de contingência

4.1.17. Assegurar a continuidade dos serviços durante eventual período de transição contratual, caso haja nova contratação em andamento, por prazo acordado com a Administração, a fim de garantir a operação ininterrupta dos serviços essenciais de tecnologia da informação.

4.1.18. Restituir, quando aplicável, equipamentos, materiais, documentos, credenciais, acessos a sistemas e demais bens disponibilizados pela contratante ao longo do contrato.

4.1.19. Emitir declaração formal de encerramento das obrigações contratuais, condicionada à aceitação pela fiscalização e à inexistência de pendências técnicas ou administrativas, comprovando a plena execução dos serviços contratados e a entrega dos produtos finais previstos. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: 5 (cinco) dias da emissão da ordem de serviço;

5.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

5.1.3. Cronograma de realização dos serviços:

5.1.4. SOLUÇÃO DE ACESSO VIA WI-FI.

5.1.5. Características da solução.

5.1.6. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

5.1.7. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

5.1.8. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

5.1.9. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução.

5.1.10. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

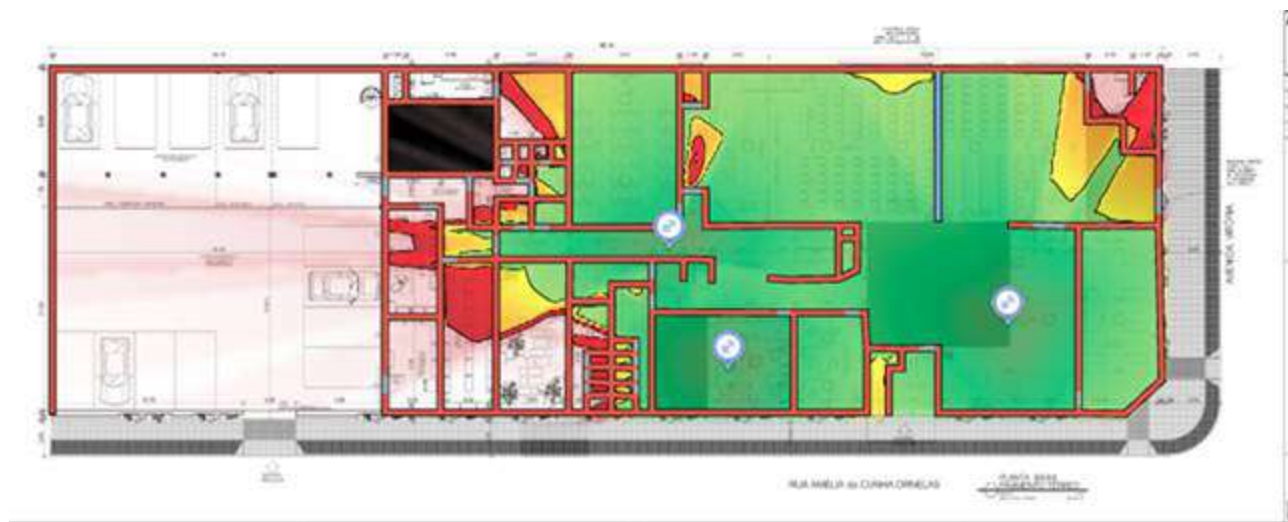
5.1.11. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

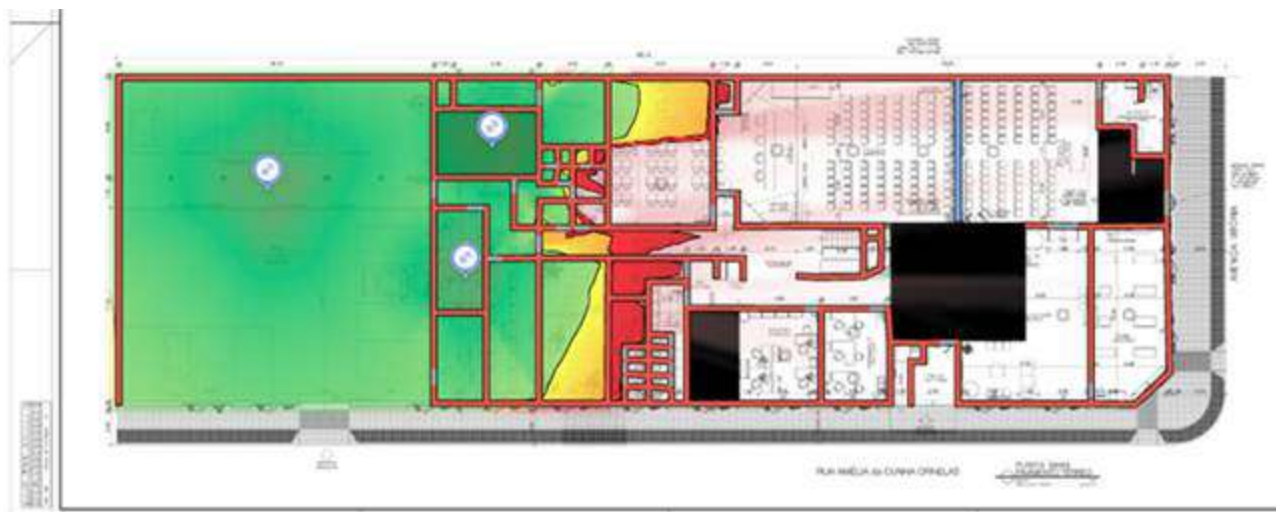
5.1.12. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.

5.1.13. Site Survey Preliminar

5.1.13.1. Para a definição da quantidade de equipamentos necessários, conforme detalhado no item 5.1.7, o CRCES realizou um levantamento de campo (site survey) preliminar, cujos resultados são apresentados a seguir:

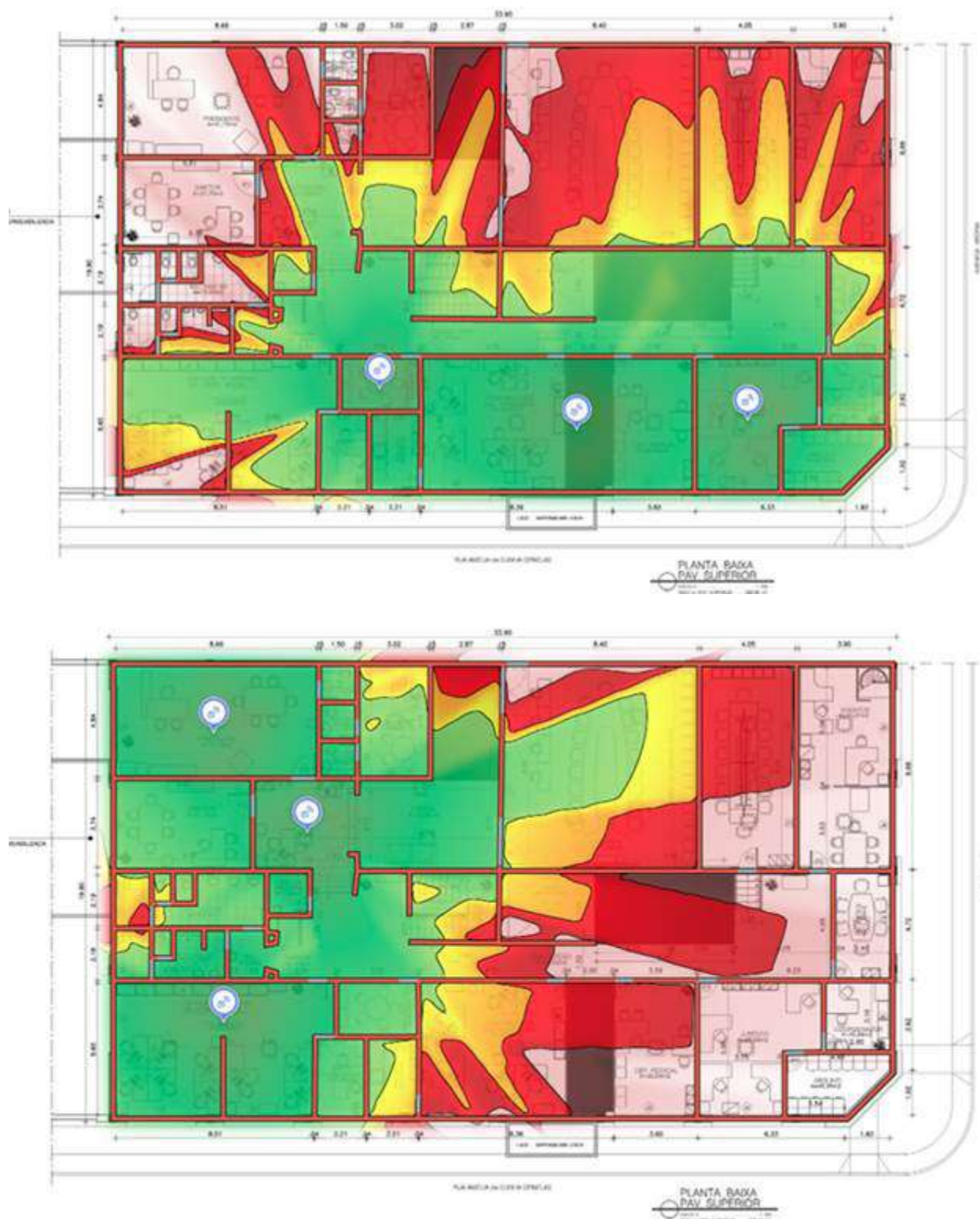
a) Pavimento térreo - 09 equipamentos





b) Pavimento superior - 09 equipamentos





5.2. Características dos pontos de acesso à internet via Wifi.

5.2.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

5.2.2. Deve ser compatível e gerenciado pelo ITENS “Firewall de Próxima Geração (NGFW) – Tipo 0x” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

5.2.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

5.2.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

5.2.5. Deve permitir ser gerenciado remotamente através de links WAN;

- 5.2.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
- 5.2.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
- 5.2.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
- 5.2.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
- 5.2.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;
- 5.2.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
- 5.2.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
- 5.2.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
- 5.2.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
- 5.2.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power Injector e adicionalmente deve possuir entrada de alimentação 12VDC;
- 5.2.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
- 5.2.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
- 5.2.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 5.2.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 5.2.20. Deve permitir operação em modo Mesh;
- 5.2.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
- 5.2.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
- 5.2.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- 5.2.24. Deve suportar OFDMA;
- 5.2.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;

- 5.2.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 5.2.27. Deve suportar BSS Coloring;
- 5.2.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- 5.2.29. Deve suportar operação em 6GHz com canais de 20, 40,80 e 160MHz;
- 5.2.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);
- 5.2.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;
- 5.2.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;
- 5.2.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
- 5.2.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 5.2.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
- 5.2.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- 5.2.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);
- 5.2.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
- 5.2.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 5.2.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 5.2.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 5.2.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 5.2.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 5.2.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 5.2.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 5.2.46. Deve implementar o padrão IEEE 802.11e;
- 5.2.47. Deve implementar o padrão IEEE 802.11h;
- 5.2.48. Deve implementar o padrão IEEE 802.3az;
- 5.2.49. Deve suportar ser gerenciado via SNMP;

5.2.50. Deve suportar consultas via REST API;

5.2.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

5.2.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

5.2.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

5.2.54. Deve possuir indicadores luminosos (LED) para indicação de status;

5.2.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

5.2.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

5.2.57. Deve possuir certificado emitido pela Wi-Fi Alliance;

5.2.58. Deve estar homologado pela ANATEL na data de execução do pregão;

5.2.59. Deve ser licenciado para uso pelo período de duração da contratação.

5.2.60. Deve possuir garantia para uso pelo período de duração da contratação.

5.2.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

5.3. Características do equipamento controlador de pontos de acesso Wifi;

5.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

5.3.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

5.3.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

5.3.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;

5.3.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

5.3.6. Deve possuir 1 (uma) interface USB;

5.3.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);

5.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

5.3.9. Deve possuir tabela MAC com suporte a 32.000 endereços;

5.3.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

5.3.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

5.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

5.3.13. Deve suportar a comutação de Jumbo Frames;

- 5.3.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz.
- 5.3.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs.
- 5.3.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6.
- 5.3.17. Deve implementar serviço de DHCP Relay.
- 5.3.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela.
- 5.3.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN).
- 5.3.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree.
- 5.3.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física.
- 5.3.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2.
- 5.3.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente.
- 5.3.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado.
- 5.3.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos.
- 5.3.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit.
- 5.3.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID.
- 5.3.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede.
- 5.3.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).
- 5.3.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.
- 5.3.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta.
- 5.3.32. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP.
- 5.3.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede.
- 5.3.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS.
- 5.3.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta.

- 5.3.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X.
- 5.3.37. Deve suportar MAC Authentication Bypass (MAB).
- 5.3.38. Deve implementar RADIUS CoA (Change of Authorization).
- 5.3.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede.
- 5.3.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado.
- 5.3.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface.
- 5.3.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP.
- 5.3.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6.
- 5.3.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema.
- 5.3.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table).
- 5.3.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface.
- 5.3.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio.
- 5.3.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog.
- 5.3.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 5.3.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface).
- 5.3.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web.
- 5.3.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS).
- 5.3.53. Deve permitir ser gerenciado através de IPv6.
- 5.3.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch.
- 5.3.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento.
- 5.3.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap.
- 5.3.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab.
- 5.3.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo,

informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo.

5.3.59. Deverá suportar ser configurado e monitorado através de REST API.

5.3.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE).

5.3.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch.

5.3.62. Deve suportar temperatura de operação de até 45º Celsius.

5.3.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.

5.3.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.

5.3.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos.

5.3.66. Deve ser licenciado para uso pelo período de duração da contratação.

5.3.67. Deve possuir garantia para uso pelo período de duração da contratação.

5.3.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

5.4. Requisitos da instalação dos pontos de acesso à internet via Wifi

5.4.1. Requisitos para instalação do item 5.3

5.4.2. Serviço de Implementação para rede WLAN

5.4.3. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura 3 total, sendo observada a quantidade mínima estabelecida pela DTIC.

5.4.4. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE.

5.4.5. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço.

5.4.6. Requisitos gerais de Implantação

5.4.7. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.

5.4.8. Instalação física

5.4.9. Será realizada instalação física conforme a necessidade da contratante.

5.4.10. O ponto de acesso wifi deverá ser fixado no teto ou parede.

5.4.11. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

5.5. Implementação lógica

5.5.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir

5.5.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela

plataforma de gerenciamento unificado.

5.5.3. Cadastro das subscrições dos APs na plataforma de gerência.

5.5.4. Endereçamento e segmentação das Redes WIRELESS.

5.5.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless.

5.5.6. Definição de políticas de bloqueio e permissão de acesso.

5.5.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante.

5.5.8. Configuração de Endereços/Interfaces de Gerência:

5.5.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),

5.5.10. Parâmetros SNMP para monitoração/gerência remota.

5.5.11. Configuração de Syslog, quando aplicável.

5.5.12. Configuração de redes locais (VLANs).

5.5.13. Configuração de redes locais (SSIDs).

5.5.14. Configuração de sincronismo de hora NTP ou SNTP.

5.5.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.

5.5.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável.

5.5.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido.

5.5.18. Configurações de grupos de ponto de acesso.

5.5.19. Configuração de algoritmo de criptografia a ser utilizado.

5.5.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido.

5.5.21. Identificar os pontos de acesso por localização conforme survey realizado.

5.5.22. Configuração de segurança de rede.

5.5.23. Realizar testes de desempenho de RF dos pontos de acesso wireless.

5.5.24. Adequar o posicionamento de pontos de acesso da solução instalada.

5.5.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento.

5.5.26. Emissão de relatórios de implantação contendo:

5.5.27. Mapas de rede,

5.5.28. Relação de equipamentos implantados,

5.5.29. Configurações feitas nos softwares;

5.5.30. Resultado dos testes realizados.

5.6. Requisitos para instalação do controlador de pontos de acesso Wifi

5.6.1. Todo o processo de instalação será precedido de um estudo e entendimento de toda a infraestrutura em funcionamento hoje no ambiente englobando sua topologia, todas as configurações em uso (endereçamentos IP, VLANs, rotas, QoS, ACL's, etc).

5.6.2. Para a implementação da solução bem como acompanhamento do projeto proposto, a licitante deverá apresentar profissionais certificados, níveis avançados de conhecimento nas tecnologias ofertados e necessárias para implantação da solução proposta.

5.6.3. O serviço de instalação, configuração da rede precederá de um cronograma de projeto para implementação das ações abaixo descritas, a ser elaborado de comum acordo.

5.6.4. Todo serviço deverá ser realizado por profissional do fabricante ou certificado por ele para execução dos serviços, para isso deverá ser apresentado junto com a proposta o certificado do profissional que irá executar os serviços de implantação.

5.6.5. Planejamento e Projeto para Instalação da Solução

5.6.6. Levantamento e análise da configuração atual da rede.

5.6.7. Elaboração de Projeto de Rede detalhado em conjunto com a equipe de tecnologia da informação, incluindo os itens de configuração a seguir:

5.6.8. Endereçamento e segmentação das Redes LAN e WAN;

5.6.9. Roteamento estativo e dinâmico utilizando protocolos RIPv2 e OSPFv2, se aplicável;

5.6.10. Qualidade de Serviço (QoS): regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede.

5.6.11. **Segurança:**

5.6.12. Dos ativos: protocolos de comunicação segura, autenticação para acesso e proteção contra-ataques.

5.6.13. Da rede: controles a serem implementados para restringir o acesso à rede e reduzir a exposição dos servidores e estações de trabalho.

5.6.14. **Instalação da Solução**

5.6.15. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos.

5.6.16. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal.

5.6.17. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante.

5.6.18. Configuração de Endereços/Interfaces de Gerência.

5.6.19. Endereçamento IP.

5.6.20. Telnet, se necessário.

5.6.21. Secure Shell (SSH), se necessário.

5.6.22. Web (HTTP), se necessário.

5.6.23. Restrições (Filtros/ACLs) de Acesso.

5.6.24. Autenticação.

5.6.25. Parâmetros SNMP para monitoração/gerência remota.

5.6.26. Configuração de redes locais (VLANs).

5.6.27. Configuração de sincronismo de hora NTP ou SNTP.

5.6.28. Configuração do protocolo Rapid Spanning Tree (RSTP).

5.6.29. Configuração de BPDU GUARD.

5.6.30. Configuração de Root Spanning Tree.

5.6.31. Interfaces de roteamento IP.

5.6.32. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado.

5.6.33. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável.

5.6.34. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado.

5.7. Otimização da Solução

5.7.1. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

5.7.2. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido.

5.7.3. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto.

5.7.4. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto.

5.7.5. Ativação de recursos para o controle de broadcast storms.

5.7.6. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado.

5.7.7. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido.

5.7.8. Controle de acesso a rede através do padrão IEEE 802.1x.

5.7.9. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento.

5.7.10. Configuração de DHCP Snooping.

5.7.11. Configuração de DHCP Relay.

5.7.12. Configuração de interface confiável (trust Interface).

5.7.13. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.

5.7.14. Configurações dos perfis de acesso à rede baseadas na Política de Segurança.

5.7.15. Criação e ativação de regras de acesso e perfis de acesso à rede.

5.7.16. Configuração de parâmetros de qualidade de serviço (QoS).

5.7.17. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente.

5.7.18. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos.

5.7.19. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política.

5.7.20. Ativação e teste das ACLs nos equipamentos fornecidos.

5.8. Homologação

5.8.1. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.

5.8.2. Documentação em formato PDF contendo os itens a seguir:

5.8.3. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.

5.8.4. Arquivos de configuração dos ativos de rede.

5.8.5. Backup das configurações dos softwares utilizados.

5.8.6. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega.

5.9. Requisitos para instalação do cabeamento

5.9.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE.

5.9.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida.

5.9.3. Conectorização e crimpagem dos cabos em ambos os extremos.

5.9.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso.

5.9.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal.

5.9.6. Teste de continuidade e certificação com laudo de todos os pontos instalados.

5.9.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606.

5.9.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

5.10. Descrição do suporte continuado

5.10.1. A CONTRATADA deverá prestar assistência em horário comercial, das 07:30 às 16:30h na modalidade 8x5.

5.10.2. A CONTRATADA deverá providenciar a imediata reposição de equipamentos que estejam indisponíveis, seja por manutenção preventiva, seja por manutenção corretiva, avarias, acidentes ou paralisados por falhas provocadas por falta de suprimento, no prazo máximo de 24 (vinte e quatro) horas.

5.10.3. Da Manutenção Preventiva A Contratada é a única e exclusiva responsável pela manutenção preventiva dos equipamentos objeto desta contratação; A manutenção deve obedecer às recomendações do fabricante de cada equipamento, porém, sem se limitar a elas e aos serviços abaixo descritos:

5.10.4. Providenciar revisão geral de todos os itens previstos de acordo com a recomendação do fabricante.

5.10.5. Verificar o estado geral de conservação dos equipamentos e providenciar substituição dos mesmos sempre que for necessário.

5.10.6. Efetuar as revisões periódicas, observando as recomendações do fabricante.

5.10.7. A Contratada deverá realizar as manutenções preventivas para garantir o pleno funcionamento dos equipamentos e a qualidade dos materiais produzidos.

5.11. Manutenção Corretiva

5.11.1. A manutenção corretiva deverá ocorrer sempre que a substituição do equipamento for necessária por quebra, assim como quando surgirem falhas.

5.11.2. A CONTRATADA deverá iniciar a manutenção corretiva em um prazo máximo de 4 (quatro) horas após a notificação por parte da CONTRATANTE, respeitando os horários definidos pela CONTRATANTE para essa tarefa.

5.11.3. A CONTRATADA deverá arcar com todos os custos decorrentes de avarias, exceto os decorrentes do mau uso do equipamento por parte do Contratante; Nesses casos, será de responsabilidade do Contratante arcar com os custos de reparo do equipamento.

5.11.4. A CONTRATADA deverá assumir integral e absoluta responsabilidade pelos equipamentos locados, desobrigando a CONTRATANTE de qualquer ônus, encargos, deveres e responsabilidade por defeitos, vícios aparentes ou ocultos, ou funcionamento insatisfatório dos aludidos bens e acidentes.

5.12. Serviço continuado

5.12.1. CONTRATADA deverá assumir a responsabilidade pelo gerenciamento da WLAN no que tange as seguintes ações:

5.12.2. Provisionamento e descoberta de dispositivos.

5.12.3. Prestar suporte técnico remoto e presencial.

- 5.12.4. Realizar atualizações de firmware e patches de segurança nos equipamentos.
- 5.12.5. Fazer a gestão de capacidade, espectro e canais da rede wireless.
- 5.12.6. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 5.12.7. Monitorar continuamente a saúde dos dispositivos.
- 5.12.8. Monitorar perfil de usuário.
- 5.12.9. Monitorar Autenticação de usuários.
- 5.12.10. Proteção e implementação de WLAN usando os protocolos de segurança descritos no TR.
- 5.12.11. Entregar relatórios mensais com análise de disponibilidade, uso de canais, desempenho e incidentes.
- 5.12.12. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 5.12.13. Corrigir falhas em conectores, cabos, patch panels e pontos RJ45 usados na solução.
- 5.13. ITEM - FIREWALL (SEDE)
 - 5.13.1. Características da solução
 - 5.13.2. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
 - 5.13.3. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
 - 5.13.4. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
 - 5.13.5. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
 - 5.13.6. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução.
 - 5.13.7. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.
 - 5.13.8. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.
 - 5.13.9. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.
- 5.14. Requisitos técnicos dos equipamentos que compõe a solução
 - 5.14.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote.
 - 5.14.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas.
 - 5.14.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo.

- 5.14.4. Deve Suportar, no mínimo, 6,5 (Seis virgula cinco) Gbps de throughput VPN IPSec.
- 5.14.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos.
- 5.14.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos.
- 5.14.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS.
- 5.14.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL.
- 5.14.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.
- 5.14.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB.
- 5.14.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB.
- 5.14.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento.
- 5.14.13. Deve possuir porta console RJ-45.
- 5.14.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance.
- 5.14.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.
- 5.14.16. Deve possuir Fontes redundantes.
- 5.14.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.
- 5.14.18. Deve ser licenciado para uso pelo período de duração do contrato.
- 5.14.19. Deve possuir garantia para uso pelo período de duração do contrato.
- 5.15. Firewalls de próxima geração (NGFW)
- 5.15.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
- 5.15.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- 5.15.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.
- 5.15.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos.
- 5.15.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação.
- 5.15.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.
- 5.16. Funcionalidades de rede e firewall
- 5.16.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

- 5.16.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans.
- 5.16.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).
- 5.16.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay.
- 5.16.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.
- 5.16.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT.
- 5.16.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- 5.16.8. Deverá suportar sFlow ou Netflow.
- 5.16.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas.
- 5.16.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual.
- 5.16.11. Deve suportar o protocolo padrão da indústria VXLAN.
- 5.16.12. Deve implementar o protocolo ECMP.
- 5.16.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança.
- 5.16.14. Enviar log para sistemas de monitoração externos.
- 5.16.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL.
- 5.16.16. Deve possuir mecanismos de proteção anti-spoofing.
- 5.16.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2).
- 5.16.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- 5.16.19. Suportar OSPF graceful restart.
- 5.16.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
- 5.16.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
- 5.16.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.
- 5.16.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo.
- 5.16.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB.
- 5.16.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões.
- 5.16.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link.
- 5.16.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática.
- 5.16.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes.
- 5.16.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de

configuração e ocorrência de eventos de rede e segurança pré-definidos.

5.16.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores.

5.16.31. Deverá suportar controle por zonas de segurança.

5.16.32. Deverá suportar controles de políticas por porta e protocolo.

5.16.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações.

5.16.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.16.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU).

5.16.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound).

5.16.37. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3.

5.16.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.

5.16.39. Suporte a objetos e regras IPV6.

5.16.40. Suporte a objetos e regras multicast.

5.16.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

5.17. Funcionalidade de controle de aplicações

5.17.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.17.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.17.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

5.17.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações.

5.17.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote e google-docs.

5.17.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo.

5.17.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

5.17.8. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.17.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.

5.17.10. Identificar o uso de táticas evasivas via comunicações criptografadas.

5.17.11. Atualizar a base de assinaturas de aplicações automaticamente.

5.17.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de

rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

5.17.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

5.17.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

5.17.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante.

5.17.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.17.17. Deve alertar o usuário quando uma aplicação for bloqueada.

5.17.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.

5.17.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.

5.17.20. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD.

5.17.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.

5.17.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

5.17.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade.

5.17.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

5.17.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

5.18. Funcionalidade de prevenção de intrusão de ameaças.

5.18.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

5.18.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

5.18.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

5.18.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e “quarentenar” IP do atacante por um intervalo de tempo.

5.18.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

5.18.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

5.18.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

5.18.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a

criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

5.18.9. Deve permitir o bloqueio de vulnerabilidades.

5.18.10. Deve permitir o bloqueio de exploits conhecidos.

5.18.11. Deve incluir proteção contra-ataques de negação de serviços.

5.18.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.18.13. Detectar e bloquear a origem de portscans.

5.18.14. Bloquear ataques efetuados por worms conhecidos.

5.18.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

5.18.16. Possuir assinaturas para bloqueio de ataques de buffer overflow.

5.18.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

5.18.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

5.18.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

5.18.20. Identificar e bloquear comunicação com botnets.

5.18.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.18.22. Os eventos devem identificar o país de onde partiu a ameaça.

5.18.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

5.18.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

5.18.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

5.18.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante.

5.18.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

5.18.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

5.19. Funcionalidade de filtro de conteúdo web e dns

5.19.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

5.19.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança.

5.19.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

5.19.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar

através da solução.

5.19.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

5.19.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.

5.19.7. Possuir pelo menos 70 (setenta) categorias de URLs.

5.19.8. Deve possuir a função de exclusão de URLs do bloqueio.

5.19.9. Permitir a customização de página de bloqueio.

5.19.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados.

5.19.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário.

5.19.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas.

5.19.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado.

5.20. Funcionalidade de identificação de usuários

5.20.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local.

5.20.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.20.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior.

5.20.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários.

5.20.5. Deve possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.20.6. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

5.20.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.20.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

5.20.9. Deve suportar o envio e recebimento de credenciais via RADIUS.

5.20.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

5.21. Funcionalidade de filtro de dados

5.21.1. Permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP).

5.21.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

5.21.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

5.21.4. Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

5.22. Funcionalidade de geolocalização

5.22.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados.

5.22.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.23. Funcionalidade de VPN

5.23.1. Suportar VPN Site-to-Site e Cliente-To-Site.

5.23.2. Suportar IPSec VPN.

5.23.3. A VPN IPSEC deve suportar 3DES.

5.23.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1.

5.23.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.23.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

5.23.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).

5.23.8. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI.

5.23.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

5.23.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6.

5.23.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.23.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.23.13. Atribuição de DNS nos clientes remotos de VPN.

5.23.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

5.23.15. Suportar autenticação via AD/LDAP, certificado e base de usuários local.

5.23.16. Suportar leitura e verificação de CRL (Certificate Revocation List).

5.23.17. Deverá manter uma conexão segura com o portal durante a sessão.

5.23.18. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

5.24. Funcionalidade de QoS, Traffic Shaping e priorização de tráfego

5.24.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

5.24.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

5.24.3. Endereço de origem e Endereço de destino.

5.24.4. Usuário e grupo.

5.24.5. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

5.24.6. Por porta.

5.24.7. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio.

5.24.8. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros.

5.24.9. O QoS deve possibilitar a definição de fila de prioridade.

5.24.10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

5.24.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação.

5.24.12. Suportar modificação de valores DSCP para o Diffserv.

5.24.13. Suportar priorização de tráfego usando informação de ToS (Type of Service).

5.24.14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.

5.24.15. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes.

5.24.16. Deve possibilitar a definição de bandas distintas para download e upload.

5.25. Funcionalidade de balanceamento inteligente de links

5.25.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.

5.25.2. A solução deve ser capaz de agregar vários links em uma interface virtual.

5.25.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc).

5.25.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente.

5.25.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada.

5.25.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score).

5.25.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

5.25.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

5.25.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

5.25.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda.

5.25.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface

está conectada.

5.25.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada.

5.25.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado.

5.25.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+).

5.25.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc).

5.25.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos.

5.25.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede.

5.25.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações.

5.25.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito.

5.25.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários.

5.25.21. A solução deve suportar nativamente conectores com clouds públicas.

5.25.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload.

5.25.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência).

5.25.24. Deve implementar balanceamento de link por hash do IP de origem.

5.25.25. Deve implementar balanceamento de link por hash do IP de origem e destino.

5.25.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links.

5.25.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal.

5.25.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

5.26. Funcionalidade de controlador de rede sem fio

5.26.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

5.26.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE

802.11a/b/g/n/ac/ax.

5.26.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6.

5.26.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet.

5.26.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS.

5.26.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário.

5.26.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points.

5.26.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso.

5.26.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec.

5.26.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção.

5.26.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless.

5.26.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X.

5.26.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso.

5.26.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz.

5.26.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.

5.26.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.

5.26.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso.

- 5.26.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados.
- 5.26.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN.
- 5.26.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados.
- 5.26.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless.
- 5.26.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária.
- 5.26.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP.
- 5.26.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado.
- 5.26.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários.
- 5.26.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio.
- 5.26.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming.
- 5.26.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming.
- 5.26.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos.
- 5.26.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless.
- 5.26.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada.
- 5.26.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas.
- 5.26.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de

acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação.

5.26.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering.

5.26.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados.

5.26.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime.

5.26.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso.

5.26.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados.

5.26.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados.

5.26.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz.

5.26.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs.

5.26.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências.

5.26.43. A solução deve ser capaz de implementar regras de firewall stateful para controlar o tráfego, permitindo ou descartando pacotes de acordo com a política configurada. Essas regras devem usar como critérios: dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos.

5.26.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego.

5.26.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS.

5.26.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES).

5.26.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3.

5.26.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID.

5.26.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada.

5.26.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS.

5.26.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X.

5.26.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP.

- 5.26.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede.
- 5.26.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless.
- 5.26.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens.
- 5.26.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede.
- 5.26.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo.
- 5.26.58. A solução deve permitir a configuração do captive portal com endereço IPv6.
- 5.26.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada.
- 5.26.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução.
- 5.26.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado.
- 5.26.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes.
- 5.26.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN.
- 5.26.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless.
- 5.26.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado.
- 5.26.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados.
- 5.26.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor.
- 5.26.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados.
- 5.26.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6.
- 5.26.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos.
- 5.26.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps.
- 5.26.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP.
- 5.26.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet like MIB).
- 5.26.74. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap.
- 5.26.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a

adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD.

5.26.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles.

5.26.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas.

5.26.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente.

5.26.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica.

5.26.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes.

5.26.81. A solução deve possuir ferramentas de diagnósticos e debug.

5.26.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso.

5.26.83. A solução deve suportar comunicação com elementos externos através de REST API.

5.26.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo.

5.27. Funcionalidade de controlador de rede cabeada

5.27.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

5.27.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.

5.27.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.

5.27.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.

5.27.5. Deve montar a topologia da rede de maneira automática.

5.27.6. Deve ser capaz de configurar os switches da rede.

5.27.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados.

5.27.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches.

5.27.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches.

5.27.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches.

5.27.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches.

5.27.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches.

5.27.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.

5.27.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.

5.27.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).

5.27.16. Deve ser capaz de configurar parâmetros SNMP dos switches.

5.27.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.

5.27.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.

5.27.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica.

5.27.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches.

5.27.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.

5.27.22. Deve prover indicadores de saúde dos elementos críticos do ambiente.

5.27.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.

5.27.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

5.28. Serviço de instalação firewall

5.28.1. Instalação Estrutura Física

5.28.2. Levantamento de toda estrutura física do ambiente.

5.28.3. Levantamento da estrutura Elétrica.

5.28.4. Verificação do espaço a ser instalado os equipamentos.

5.28.5. Abertura e conferência das caixas dos equipamentos.

5.28.6. Instalação do appliance físico

5.28.7. Fixação do equipamento no RACK.

5.28.8. Conexão da fonte de alimentação elétrica em régua de tomada.

5.28.9. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento.

5.28.10. Conexão das interfaces de rede com os switches.

5.28.11. Configuração do appliance físico

5.28.12. Parametrização do Licenciamento.

5.28.13. Parametrização das interfaces de rede.

5.28.14. Atualização da última versão de Firmware.

5.28.15. Parametrização das regras de NAT.

5.28.16. Parametrização do Filtro de Conteúdo (WebFilter).

5.28.17. Parametrização de Controle de Aplicação.

5.28.18. Parametrização de VPN (Virtual Private Network).

5.28.19. Parametrização IDS/IPS.

5.28.20. Parametrização DNS.

5.28.21. Parametrização de Gateway Antivírus.

5.28.22. Parametrização de Objetos de Endereço.

5.28.23. Parametrização de Grupo de Objetos.

5.28.24. Parametrização de Load Balancing.

5.28.25. Parametrização de SSO (Single Sing-on).

5.28.26. Parametrização de SNMP.

5.28.27. Parametrização de NTP.

5.28.28. Parametrização de PortGroups.

5.28.29. Parametrização de Zones.

5.28.30. Parametrização de Serviços.

5.28.31. Parametrização de Rotas.

5.28.32. Parametrização de DHCP.

5.29. Serviços profissionais de suporte técnico na solução de firewall

5.29.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5.

5.29.2. Efetuar toda rotina de backup das configurações semanalmente.

5.29.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento.

5.29.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

5.29.5. Criação das rotas para links.

5.29.6. Criação de NAT.

5.29.7. Liberação de portas.

5.29.8. Configuração do Filtro de Conteúdo.

5.29.9. Configuração do Controle de Aplicativos.

5.29.10. Configuração do Agente para autenticação LDAP.

5.29.11. Configuração para o Single Sign-On (SSO).

5.29.12. Configurações dos serviços avançados de segurança (IPS, Antivírus).

5.29.13. Configuração de VPN client to site.

5.29.14. Configuração de VPN site to site.

5.29.15. Criação de regras de Firewall.

5.29.16. Criação de regras de QoS.

5.29.17. Emitir relatório de segurança mensal por localidade.

5.29.18. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.

5.29.19. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.

5.29.20. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de

Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

5.30. SLA dos serviços e atendimento

5.30.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções.

5.30.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução.

5.30.3. Gerar relatórios de acesso e desempenho da solução de firewall.

5.30.4. Deverá possuir sistema de abertura de chamados pela internet.

5.30.5. Monitorar latência e uptime dos links configurados.

5.30.6. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:

5.30.7. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.

5.30.8. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

5.30.9. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

5.30.10. Níveis de Severidade

5.30.10.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

5.30.10.2. Para os chamados classificados como de severidade 1, a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (quatro) horas úteis após o registro do chamado.

5.30.10.3. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

5.30.10.4. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.30.10.5. Para os chamados classificados como severidade 2, a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.30.10.6. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

5.30.10.7. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.30.10.8. Para os chamados classificados como severidade 3, a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.30.10.9. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência.

5.30.10.10. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

5.30.10.11. Para os chamados classificados como severidade 4, a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.30.10.12. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

5.30.10.13. Não poderá haver limites no quantitativo de abertura de chamados.

5.30.11. Qualificação Técnica

5.30.11.1. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

5.30.11.2. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros).

5.30.11.3. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico.

5.30.11.4. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas.

5.30.11.5. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan os trechos da documentação que comprovem os

respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização.

5.30.12. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

5.30.12.1. Definição do objeto

5.30.12.2. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), aços de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (Físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, aços de rede, firewall (SonicWall), nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

5.30.12.3. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21 da Lei nº 14.133, de 2021.

5.30.12.4. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar.

5.30.12.5. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

5.30.12.6. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

5.30.12.7. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

5.30.13. Características da solução

5.30.13.1. Início da execução do objeto: 05 (cinco) dias úteis da emissão da ordem de serviço.

5.30.13.2. Descrição detalhada:

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12

02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

5.30.14. Contratada deve prestar os serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente.

5.30.15. A empresa deverá estar pronta para gerir toda a estrutura hiperconvergente, que conta atualmente com dois clusters gerenciados de forma separada (com armazenamento baseado em

Software-defined storage -SDS), uma infraestrutura com base em acessos VDI, máquinas virtuais. A empresa contratada deve estar pronta para lidar com seus backups, restores, e qualquer problema, falha, atualização, instalação ou análise oriunda desta relação de ferramentas integradas.

5.30.16. Requisitos técnicos

5.30.16.1. Monitoramento e suporte técnico

5.30.16.2. Realizar o monitoramento proativo das estações de trabalho.

5.30.16.3. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:

5.30.16.4. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns).

5.30.16.5. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos.

5.30.16.6. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos.

5.30.16.7. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

5.30.17. Manutenção, gestão de ativos e rede

5.30.17.1. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos.

5.30.17.2. Realizar gestão e manutenção da estrutura hiperconvergente.

5.30.17.3. Garantir o pleno funcionamento da solução de telefonia IP local.

5.30.17.4. Executar a gestão técnica da infraestrutura de rede, abrangendo:

5.30.17.5. Administração de lans, vlans e sub-redes.

5.30.17.6. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast.

5.30.17.7. Implementação de boas práticas para prevenção de incidentes.

5.30.17.8. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.

5.30.17.9. Executar serviços de instalação e gerenciamento de cabeamento de rede.

5.30.18. Serviços gerenciados

5.30.19. Prestar serviços gerenciados de segurança da rede e ativos de TI.

5.30.20. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores.

5.30.21. Gerenciar e administrar o ambiente de Office 365.

5.30.22. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

5.30.23. Controle, inventário e chamados

5.30.24. Manter atualizado o inventário de hardware e software.

5.30.25. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

5.30.26. Logística e apoio à contratação

5.30.27. Executar a logística de coleta e entrega de equipamentos.

5.30.28. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI.

5.30.29. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis. a partir de solicitação formal da CONTRATANTE.

5.30.30. Atendimento presencial

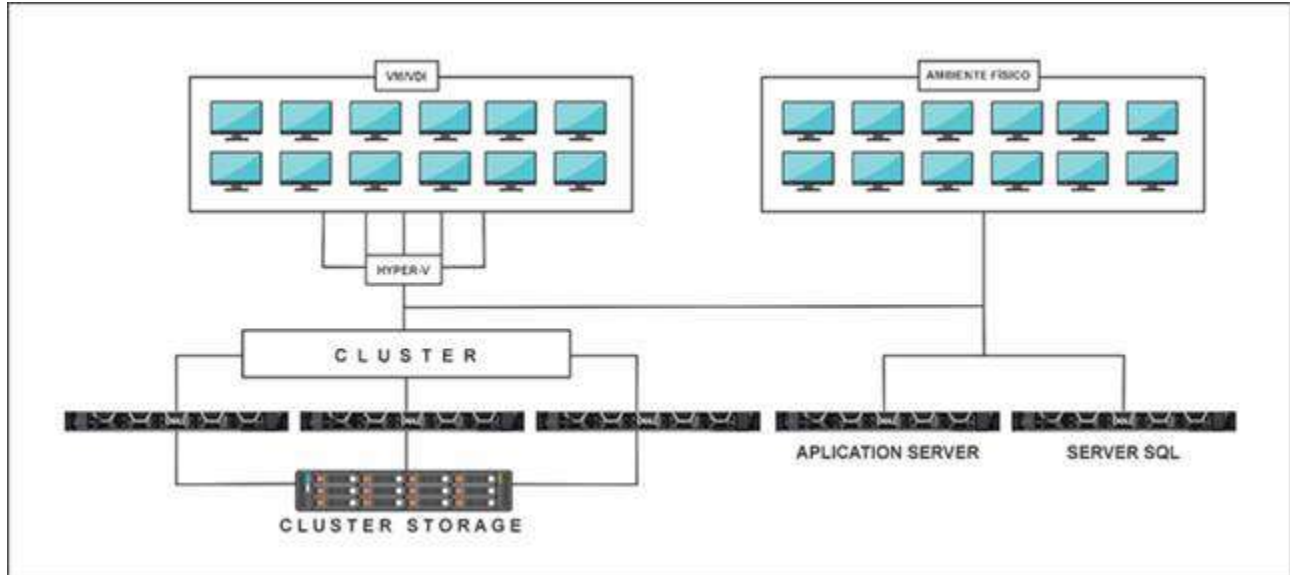
5.30.31. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 8 (oito) horas por visita.

5.30.32. Parque de informática do CRCES

TIPO	DESCRIÇÃO	QUANTIDADE
Equipamento de segurança	Firewall a ser contratado neste termo de referência	01
Pontos de acesso	Pontos de acesso a serem contratados neste termo de referência	A depender da solução contratada
Virtualizador	Hyper-V	05
Servidor Windows 2022 Server	Dell PowerEdge R640	02
Servidor Windows 2022 Server	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01
Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01
Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados - VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projektor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03

Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01

5.31.1. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



5.31.1. Manutenção preventiva e corretiva

5.31.2. Manutenção Preventiva

5.31.2.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

5.31.2.2. Tais atividades incluem, mas não se limitam a:

5.31.2.3. Verificação de funcionamento dos componentes físicos e lógicos;

5.31.2.4. Limpeza técnica interna e externa;

5.31.2.5. Aferição e calibração de dispositivos, quando aplicável;

5.31.2.6. Atualização de firmwares, BIOS e softwares;

5.31.2.7. Verificação e otimização de configurações;

5.31.2.8. Avaliação do desempenho geral e análise de logs;

5.31.2.9. Testes de funcionalidade e conectividade.

5.31.3. Os equipamentos e ativos de tecnologia que deverão ser contemplados no plano de manutenção preventiva incluem:

5.31.4. Servidores físicos;

5.31.5. Servidores virtuais;

5.31.6. Infraestrutura de rede (switches, cabeamento, racks, patch panels, etc.);

5.31.7. Ativos de rede (roteadores, access points, controladoras, etc.);

5.31.8. Estações de trabalho tipo desktop;

5.31.9. Nobreaks e sistemas de energia ininterrupta;

5.31.10. Terminais de desktop virtualizado (Thin Clients);

5.31.11. Firewalls e appliances de segurança;

5.31.12. Notebooks;

5.31.13. Scanners (digitalizadores) de mesa e portáteis;

5.31.14. Projetores multimídia;

5.31.15. Monitores LCD/LED;

5.31.16. Telefones IP e demais dispositivos de comunicação;

5.31.17. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.

5.31.18. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.

5.31.19. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.

5.31.20. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que solicitado.

5.32. Manutenção Corretiva

5.32.1. Em caso de surgimento de problema técnico em qualquer um dos equipamentos ou serviços listados no item de manutenção preventiva (item 5.1.7) a contratada deverá providenciar laudo técnico (item 6.1.3.1) e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.

5.32.2. CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.

5.32.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.

5.32.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.

5.32.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.

5.32.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 dias úteis após o recebimento dos novos equipamentos/peças.

5.32.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.

- 5.32.8. Durante a execução do serviço externo, a empresa contratada deverá:
- 5.32.9. Se responsabilizar pelo transporte dos equipamentos que serão retirados;
- 5.32.10. Providenciar termo de responsabilidade de retirada;
- 5.32.11. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.
- 5.32.12. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;
- 5.32.13. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;
- 5.32.14. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;
- 5.32.15. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;
- 5.32.16. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto à qualidade do produto entregue;
- 5.32.17. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.
- 5.33. SLA dos serviços e atendimento
- 5.33.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 5.33.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 5.33.3. O ambiente de TI do CRCES deverá ser continuamente monitorado por ferramentas especializadas, com alertas automáticos e registro de falhas, a fim de garantir o funcionamento adequado e a disponibilidade dos recursos.
- 5.33.4. deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos
- 5.33.5. Deverá possuir sistema de abertura de chamados pela internet.
- 5.33.6. Monitorar latência e uptime dos links configurados.
- 5.33.7. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 5.33.8. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 5.33.9. Os níveis de atendimento técnico (N1, N2 e N3) deverão seguir o escopo descrito no item 1.3.3.3 a 1.3.3.6, com suporte remoto ilimitado e visitas técnicas presenciais duas vezes por semana, conforme cláusula 1.3.3.34.
- 5.33.10. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 5.33.11. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade

1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.
3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup.
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

5.33.11.1. Níveis de Severidade

5.33.11.2. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

5.33.11.3. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

5.33.11.4. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

5.33.11.5. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.33.11.6. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.33.11.7. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

5.33.11.8. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.33.11.9. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.33.11.10. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

5.33.11.11. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

5.33.11.12. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.33.11.13. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

5.33.11.14. Não poderá haver limites no quantitativo de abertura de chamados.

5.34. Qualificação Técnica

5.34.1. A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a

efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se inviável:

5.34.2. Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.

5.34.3. Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.

5.34.4. Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.

5.34.5. Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.

5.34.6. Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.

5.34.7. Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.

5.34.8. Certificação ITIL v3 ou superior;

5.34.9. Certificação MCSA Windows Server 2012 ou superior;

5.34.10. A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:

5.34.11. Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;

5.34.12. Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;

5.34.13. Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

5.35. BACKUP CORPORATIVO

5.35.1.1. Software de Backup

5.35.2. Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,

5.35.3. Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.

5.35.4. Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.

5.35.5. Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.

5.35.6. Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.

5.35.7. Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho

conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.

5.35.8. Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.

5.35.9. Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.

5.35.10. Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.

5.35.11. 2.1.10. Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.

5.35.12. Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra-ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.

5.35.13. Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.

5.35.14. Backup de Máquinas Virtuais com Consistência de Aplicações: O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.

5.35.15. Backup Incremental e Diferencial: Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.

5.35.16. Cópias de Backup Imutáveis: Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.

5.35.17. Retenção Personalizável: O software deve oferecer flexibilidade na configuração de políticas de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.

5.35.18. Arquivamento Inteligente: Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.

5.35.19. Monitoramento e Alertas: O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.

5.35.20. Dashboard Intuitivo: Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.

5.35.21. Otimização de Recursos (IOPS e Throughput): O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.

5.35.22. Restauração Granular: Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.

5.35.23. Recuperação Bare-Metal: Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.

5.35.24. Testes de Restauração Automática: Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.

5.35.25. Integração Nativa com Provedores de Nuvem: Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage,

no mínimo.

5.35.26. Economia de Largura de Banda: Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.

5.35.27. Perfis de Acesso Personalizáveis: O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.

5.35.28. Controle de Acessos Granular: Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.

5.35.29. Suporte a LGPD e Outras Normas: O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.

5.35.30. Auditorias e Relatórios: Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.

5.35.31. Automatização de trabalhos de Backup: Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.

5.35.32. Integração com Ferramentas de Orquestração: Suporte para integração com ferramentas

5.35.33. de orquestração e automação (ex: scripts PowerShell, APIs).

5.35.34. Cobertura Completa: O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.

5.35.35. Recuperação Granular: Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.

5.35.36. Agendamento e Automação: A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

5.36. Appliance de Backup Local

5.36.1. A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.

5.36.2. Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.

5.36.3. Será responsável por configurar o sistema de armazenamento local do equipamento, devendo:

5.36.3.1. Criar e configurar o arranjo de discos em RAID 5;

5.36.3.2. Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);

5.36.3.3. Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas

5.36.4. Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.

5.36.5. Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:

5.36.5.1. Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;

- 5.36.5.2. Gerar e manter registros e relatórios de status dos backups locais e remotos;
- 5.36.5.3. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;
- 5.36.6. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:
 - 5.36.6.1. Acompanhamento da integridade dos discos e volumes lógicos;
 - 5.36.6.2. Monitoramento do uso de espaço em disco e alertas proativos;
 - 5.36.6.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.
- 5.36.7. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:
 - 5.36.7.1. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;
 - 5.36.7.2. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).
- 5.36.8. deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:
 - 5.36.8.1. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;
 - 5.36.8.2. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;
 - 5.36.8.3. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;
 - 5.36.8.4. Ajustar as políticas de backup e monitoramento para o novo ambiente.
- 5.36.9. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.
- 5.37. Armazenamento de backup em nuvem
 - 5.37.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.
 - 5.37.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.
 - 5.37.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.
 - 5.37.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
 - 5.37.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.
 - 5.37.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.
 - 5.37.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.
 - 5.37.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.
 - 5.37.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo

de retenção e a criticidade dos dados.

5.37.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).

5.37.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.

5.37.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.

5.37.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.

5.37.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.

5.37.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.

5.37.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.

5.37.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.

5.37.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.

5.37.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.

5.37.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).

5.37.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.

5.37.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e possíveis falhas.

5.37.23. Ferramentas de monitoramento nativas devem estar integradas.

5.37.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

5.38. SLA dos serviços e atendimento

5.38.1.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

5.38.1.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

5.38.1.3. deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime e falhas críticas.

5.38.1.4. Deverá possuir sistema de abertura de chamados pela internet.

5.38.1.5. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:

5.38.1.6. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.

5.38.1.7. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

5.38.1.8. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade	
1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.
3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup.
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

5.38.2. Níveis de Severidade

5.38.3. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

5.38.4. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

5.38.5. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

5.38.6. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.38.7. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.38.7.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

5.38.7.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.38.8. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.38.9. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

5.38.10. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

5.38.11. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

5.38.11.1. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

5.38.11.2. Não poderá haver limites no quantitativo de abertura de chamados.

5.38.12. **Certificações**

5.38.12.1. Será necessário solicitar algumas certificações, com isso o CRCES está garantindo que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade, alinhado com as melhores práticas do mercado e com as recomendações de segurança de órgãos como o NIST e o CIS.

5.38.12.2. Abaixo, vamos citar cada uma delas, ampliando as justificativas:

a) **Certificação Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 (no mínimo)**

5.38.12.3. Domínio do Sistema Operacional: A certificação MCSA garante que o profissional possui um conhecimento profundo do Windows Server 2012, que é a base do nosso ambiente corporativo hiperconvergente. Isso inclui domínio em instalação, configuração, administração e troubleshooting do sistema operacional, além de serviços como Active Directory, DNS, DHCP e outros.

5.38.12.4. Integração com Outros Serviços: O Windows Server é integrado a outros serviços da Microsoft, como Exchange, SharePoint e SQL Server. Um profissional com a certificação MCSA terá mais facilidade em integrar e gerenciar esses serviços em um ambiente unificado.

5.38.12.5. Padrão de Qualidade e Alinhamento com Boas Práticas: A certificação MCSA é reconhecida mundialmente como um padrão de qualidade para profissionais de infraestrutura. Ela demonstra que o profissional possui as habilidades necessárias para lidar com as complexidades de um ambiente como o nosso, que possui dois clusters e funciona no modelo de hiperconvergência, além de estar alinhado com as melhores práticas do mercado.

b) **Certificação para Instalação e Configuração de Switches DELL ou similar**

5.38.12.6. Infraestrutura de Rede e Otimização: Switches são equipamentos essenciais para a interconexão de dispositivos em uma rede. A certificação garante que o profissional possui conhecimento sobre os princípios de funcionamento de switches, além de saber como configurá-los para atender às necessidades específicas da rede do CRCES, que utiliza switches complexos de alta tecnologia (tanto o core quanto o de agregação da hiperconvergência). Isso permite otimizar o desempenho da rede, reduzindo a latência e aumentando a disponibilidade.

5.38.12.7. Escalabilidade e Flexibilidade: À medida que a rede cresce, é necessário adicionar novos switches. Um profissional certificado terá as habilidades necessárias para integrar novos switches à rede existente, garantindo a escalabilidade da infraestrutura e a flexibilidade para atender às futuras demandas do CRCES.

5.38.12.8. Alinhamento com as Melhores Práticas: A certificação garante que o profissional está familiarizado com as melhores práticas de configuração e gerenciamento de redes, o que contribui para a estabilidade e a segurança da infraestrutura.

5.38.12.9. As certificações solicitadas demonstram que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade para o CRCES. Elas garantem que os profissionais terão a capacidade de:

5.38.12.10. Gerenciar e manter a infraestrutura de TI de forma eficiente, segura e alinhada com as melhores práticas do mercado.

5.38.12.11. Resolver problemas de forma rápida e eficaz, minimizando o tempo de inatividade do sistema.

5.38.12.12. Implementar novas tecnologias de forma adequada e segura.

5.38.12.13. Acompanhar as melhores práticas do mercado e as recomendações de segurança de órgãos como o NIST e o CIS.

5.38.13. **Justificativa**

5.38.14. Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada para gerar todos esses serviços de TI se

torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

5.38.15. A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

5.38.16. O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a) Assegurar a contratação da empresa mais qualificada e experiente para o serviço.
- b) Definir claramente as expectativas e responsabilidades de ambas as partes.
- c) Permitir a avaliação objetiva das propostas e a escolha da melhor solução.
- d) Facilitar o acompanhamento e a fiscalização do contrato.
- e) Mitigar riscos e garantir o sucesso da contratação.
- f) Atender aos princípios da Lei 14.133 e da Administração Pública.

5.38.17. Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:

- a) Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.
- b) Aumento de custos com retrabalho, correções e possíveis perdas.
- c) Dificuldades na comunicação e na resolução de conflitos.
- d) Dificuldades na fiscalização do contrato e na cobrança de resultados.
- e) Riscos de inadimplência e de litígios.

5.38.18. A contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.

5.38.19. **Softwares que deverão ser disponibilizados**

5.38.20. As ferramentas listadas abaixo (monitoramento e de abertura de chamados) deverão ser disponibilizadas e totalmente configuradas pela CONTRATADA sem custo adicional para o CRCES, e deverão apresentar as seguintes especificações (mínimas):

5.38.21. **Ferramenta de monitoramento.**

5.38.21.1. Monitoramento de Rede: Roteadores, switches, impressoras, etc., utilizando protocolos como SNMP (v1/v2c/v3), ICMP (ping) e verificações de portas TCP/UDP.

5.38.21.2. Monitoramento de Servidores: Desempenho de CPU, uso de memória, espaço em disco, tráfego de rede, processos, serviços e logs.

5.38.21.3. Monitoramento de Aplicações e Serviços: Bancos de dados (MySQL, PostgreSQL, Oracle, etc.), servidores web (Apache, Nginx, IIS), Java applications (JMX), serviços específicos e outros.

5.38.21.4. Monitoramento de Virtualização: Serviços em nuvem, contêineres, máquinas virtuais.

5.38.21.5. Monitoramento Web (Web Scenarios): Simula a navegação de usuários em aplicações web, verificando a disponibilidade, o tempo de resposta e o conteúdo das páginas.

5.38.21.6. Monitoramento de Dispositivos IoT e Sensores: Coleta dados de uma variedade de sensores e dispositivos IoT.

5.38.21.7. Monitoramento de Logs e Eventos: Analisa arquivos de log em busca de padrões, erros, avisos ou atividades suspeitas.

5.38.21.8. Extensibilidade: Permitir a coleta de dados qualquer fonte através de scripts externos

personalizados, APIs e extensões.

5.38.21.9. Limiares Flexíveis: Definição de condições personalizadas para identificar problemas (triggers).

5.38.21.10. Previsão de Tendências e Machine Learning: Funções preditivas que permitem prever quando um limiar será atingido, possibilitando ações proativas antes que um problema ocorra.

5.38.21.11. Níveis de Severidade: Classificação dos problemas por níveis de severidade (informação, aviso, médio, alto, desastre), facilitando a priorização.

5.38.21.12. Análise de Causa Raiz: Ajuda a identificar a causa subjacente dos problemas.

5.38.21.13. Canais de Notificação Diversos: Envio de alertas por e-mail, SMS, aplicativos de mensagens (Telegram, Slack, etc.), webhooks e scripts personalizados.

5.38.21.14. Escalonamento de Alertas: Configuração de fluxos de escalonamento para garantir que os alertas cheguem aos destinatários corretos em diferentes etapas.

5.38.21.15. Ações Automáticas (Auto-remediação): Possibilidade de executar comandos remotos automaticamente em resposta a um problema (ex: reiniciar um serviço, executar um script de correção).

5.38.21.16. Notificações Customizáveis: Mensagens de alerta personalizadas com informações relevantes sobre o problema.

5.38.21.17. Dashboards Personalizáveis: Criação de painéis de controle interativos com widgets para exibir métricas em tempo real, status de hosts, problemas, mapas de rede, gráficos e muito mais.

5.38.21.18. Gráficos Flexíveis: Geração de gráficos detalhados para visualizar dados históricos e tendências, com opções de personalização de tempo e exibição.

5.38.21.19. Mapas de Rede (Network Maps): Criação de representações visuais da infraestrutura, mostrando o status dos dispositivos e as interconexões.

5.38.21.20. Relatórios: Geração de relatórios de disponibilidade, desempenho e outros dados relevantes.

5.38.21.21. Visão de Negócio (SLA/KPI): Possibilidade de monitorar o desempenho dos serviços de TI em relação aos Acordos de Nível de Serviço (SLAs) e Indicadores Chave de Desempenho (KPIs).

5.38.21.22. Descoberta Automática de Rede (Network Discovery): Detecta automaticamente novos dispositivos na rede, facilitando a configuração inicial.

5.38.21.23. Auto-registro de Agentes (Agent Autoregistration): Permite que os agentes Zabbix se registrem automaticamente no servidor Zabbix, simplificando a implantação em grande escala.

5.38.21.24. Descoberta de Baixo Nível (Low-Level Discovery - LLD): Descobre automaticamente componentes de um host (ex: interfaces de rede, sistemas de arquivos, CPUs, partições de disco) e cria itens de monitoramento, triggers e gráficos para eles.

5.38.21.25. Modelos (Templates): Reutilização de configurações de monitoramento para diferentes tipos de hosts, agilizando a implantação e padronizando o monitoramento.

5.38.21.26. Sistema de Permissões: Controle granular de acesso baseado em funções e grupos de usuários.

5.38.21.27. Autenticação: Suporte a diferentes métodos de autenticação (interna, LDAP, SAML).

5.38.22. Criptografia: Criptografia de todo o tráfego de monitoramento para garantir a segurança dos dados.

5.38.23. Alta Disponibilidade: Monitoramento contínuo.

5.39. Ferramenta de abertura e gestão de chamados de T.I

5.39.1. Abertura de chamados por e-mail: Integração com e-mail para que os chamados sejam criados automaticamente a partir de mensagens enviadas para um endereço específico.

- 5.39.2. Categorização e Priorização Automática: Possibilidade de pré-definir categorias (ex: "Problema de Software", "Solicitação de Hardware", "Acesso"), subcategorias e níveis de prioridade (ex: "Baixa", "Média", "Alta", "Crítica") com base no tipo de solicitação ou no usuário.
- 5.39.3. Anexos: Capacidade de anexar arquivos (screenshots, logs, documentos) para fornecer mais contexto ao chamado.
- 5.39.4. Atribuição Automática e Manual: Atribuição de chamados a agentes ou equipes com base em regras predefinidas (categoria, prioridade, departamento do usuário) ou atribuição manual pelos gerentes.
- 5.39.5. Filas de Atendimento: Organização dos chamados em filas específicas para cada equipe ou tipo de serviço.
- 5.39.6. Fluxos de Trabalho (Workflows): Definição de etapas e ações automatizadas para o ciclo de vida de um chamado (ex: Aberto -> Em Andamento -> Aguardando Usuário -> Resolvido -> Fechado).
- 5.39.7. Notificações Automáticas: Envio de e-mails ou notificações push para o usuário e para os agentes sobre o status do chamado, novas mensagens, resolução, etc.
- 5.39.8. Colaboração em Equipe: Permite que múltiplos agentes trabalhem em um mesmo chamado, com compartilhamento de informações e anotações.
- 5.39.9. Macros/Respostas Predefinidas: Modelos de respostas para perguntas frequentes, agilizando o atendimento.
- 5.39.10. Artigos e FAQs: Repositório central de artigos de solução de problemas, FAQs (perguntas frequentes), guias e procedimentos.
- 5.39.11. Busca Inteligente: Ferramenta de busca robusta que permite aos usuários e agentes encontrar informações relevantes rapidamente.
- 5.39.12. Sugestão de Soluções: Apresentar artigos da base de conhecimento aos usuários enquanto eles digitam seu problema no portal self-service, incentivando a auto-resolução.
- 5.39.13. Dashboards e Métricas: Visualização em tempo real de KPIs (Key Performance Indicators) como número de chamados abertos, chamados resolvidos, tempo médio de resposta, tempo médio de resolução, etc.
- 5.39.14. Relatórios Customizáveis: Geração de relatórios sobre desempenho da equipe, tipos de chamados mais comuns, cumprimento de SLAs, tendências, etc.
- 5.39.15. Integração com a ferramenta de Monitoramento: Integração com a ferramenta de monitoramento proposto pela CONTRATADA, para que alertas de monitoramento possam gerar chamados automaticamente.
- 5.39.16. Controle de Acesso Baseado em Funções: Definição de permissões diferentes para usuários, agentes e administradores.
- 5.39.17. Acessibilidade: Interface amigável e acessível em diferentes dispositivos (desktop, mobile).
- 5.39.18. SLA (Service Level Agreement) Management:
- 5.39.19. Definição de SLAs para diferentes tipos de chamados, especificando tempo de resposta e tempo de resolução esperados.
- 5.39.20. Monitoramento automático do cumprimento dos SLAs, com alertas e escalonamentos caso os prazos estejam sendo excedidos.
- 5.39.21. Escalonamento automático para gerentes ou equipes superiores quando os SLAs estão em risco.
- 5.39.22. Histórico Completo do Chamado: Registro detalhado de todas as interações, atualizações, comentários e mudanças de status em um chamado.
- 5.39.23. Pesquisa Avançada: Facilidade para buscar chamados por ID, usuário, categoria, palavras-

chave, etc.

5.40. Serviços externos que deverão ser acompanhados pela contratada

5.40.1. A CONTRATADA será um ponto focal e estratégico para o CRCES, atuando como o principal elo de coordenação e intermediação entre nossa instituição e as demais prestadoras de serviços de TI. Dada a complexidade e a interdependência de nossas operações tecnológicas, a intervenção e o acompanhamento proativo da CONTRATADA serão cruciais para garantir a fluidez e a eficácia de todas as interações e projetos. Atualmente, gerenciamos diversos contratos com terceiros, e essa carteira de fornecedores poderá se expandir conforme nossas necessidades evoluírem. Abaixo vamos listar alguns dos contratos:

- Serviço de fornecimento de software de gestão integrada (SpiderWare);
- Serviço de hospedagem do website e webservice do CRCES;
- Serviço de fornecimento de link de internet;
- Serviço de fornecimento de e-mail corporativo;
- Serviço de fornecimento de link SIP Trunk;
- Serviço de fornecimento de validador de assinaturas digitais;
- Serviço de fornecimento de atendendente virtual por whatsapp;
- Serviço de outsourcing de impressão;
- Serviço de fornecimento de ePABX;

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O CRCES poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato, o CRCES poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.6. Preposto

6.6.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.7. Fiscalização

6.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

6.7.2. O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.7.3. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

6.7.4. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.7.5. O fiscal do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

6.7.6. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

6.7.7. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

6.7.8. O fiscal do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.7.9. Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

6.8. Gestor do Contrato

6.8.1. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.8.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.8.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.8.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.8.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.8.6. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.8.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. A avaliação da execução do objeto utilizará o relatório/checklist para atesto de notas fiscais para aferição da qualidade da prestação do serviço.

7.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.1.1.1. não produzir os resultados acordados,

7.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.1.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7.1.3. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

7.1.3.1. A avaliação da execução do objeto será conduzida utilizando o instrumento de verificação de conformidade, em conformidade com as especificações técnicas estabelecidas no item 5.

7.2. Do recebimento

7.2.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. ([Art. 140, I, a, da Lei nº 14.133, de 2021](#) e [Arts. 22, X e 23, X do Decreto nº 11.246, de 2022](#)).

7.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.2.3. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências. ([Art. 22 e 23, X, Decreto nº 11.246, de 2022](#)).

7.2.4. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.2.5. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.2.6. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. ([Art. 119 c/c art. 140 da Lei nº 14133, de 2021](#))

7.2.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.2.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as

especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.2.10. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.2.11. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.2.11.1. Emitir documento comprobatório da avaliação realizada pelos fiscais, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento ([art. 21, VIII, Decreto nº 11.246, de 2022](#)).

7.2.11.2. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.2.11.3. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.2.12. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do [art. 143 da Lei nº 14.133, de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.2.13. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.2.14. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.3. Liquidação

7.3.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de cinco dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do [art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022](#).

7.3.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#).

7.3.3. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.3.3.1. o prazo de validade;

7.3.3.2. a data da emissão;

7.3.3.3. os dados do contrato e do órgão contratante;

7.3.3.4. o período respectivo de execução do contrato;

7.3.3.5. o valor a pagar; e

7.3.3.6. eventual destaque do valor de retenções tributárias cabíveis.

7.3.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

7.3.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da

regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

7.3.6. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

7.3.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.3.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.3.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.3.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

7.4. Prazo de pagamento

7.4.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.5. Forma de pagamento

7.5.1. O pagamento será realizado preferencialmente por meio de chave pix indicada pelo fornecedor, desde que a conta para pagamento esteja em nome da empresa contratada, ou através de boleto/fatura emitido por este.

7.5.1.1. Na impossibilidade de pagamento via chave pix ou boleto/fatura, o valor poderá ser transferido para conta bancária, desde que a mesma esteja em nome da empresa contratada.

7.5.2. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.5.3. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.5.4. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

8.1. Forma de seleção e critério de julgamento da proposta.

8.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

8.2. Regime de execução

8.2.1. O regime de execução do objeto será empreitada por preço **global**.

8.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

8.3.1. **Habilitação jurídica**

8.3.1.1. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.3.1.2. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

8.3.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.3.1.4. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

8.3.1.5. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.3.1.6. **Filial, sucursal ou agência de sociedade simples ou empresária :** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

8.3.1.7. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.3.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

8.3.2. **Habilitação fiscal, social e trabalhista**

8.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.3.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.3.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.3.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.3.2.5. Prova de inscrição no cadastro de contribuintes Estadual/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.3.2.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.3.2.7. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.3.2.8. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de

declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.3.2.9. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

8.3.3. Qualificação Econômico-Financeira

8.3.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

8.3.4. Qualificação Técnica

8.3.4.1. Comprovação de aptidão para a prestação de serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

8.3.4.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

8.3.4.2. Prestação de serviços de backup em nuvem com volume mínimo disponibilizado de 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável.

8.3.4.2.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

8.3.4.2. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

8.3.4.3. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

8.3.4.4. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

8.3.4.5. (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

8.3.4.6. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

8.3.4.7. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas;

8.3.4.8. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan os trechos da documentação que comprovem os respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização;

8.3.4.9. A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se

inviável:

8.3.4.10. Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.

8.3.4.11. Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.

8.3.4.13. Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.

8.3.4.12. Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.

8.3.4.13. Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.

8.3.4.14. Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.

8.3.4.15. Certificação ITIL v3 ou superior;

8.3.4.16. Certificação MCSA Windows Server 2012 ou superior;

8.3.4.19. A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:

8.3.4.20. Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;

8.3.4.21. Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;

8.3.4.22. Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

8.3.4.23. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

8.3.4.23.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.3.4.23.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.3.4.23.3. A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual;

8.3.4.23.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

8.3.4.23.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

8.3.4.23.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados

autorizaram a cooperativa a contratar o objeto da licitação;

8.3.4.23.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

8.3.4.23.8. Modelo de gestão operacional, conforme art. 10, § 1º, da IN SEGES/ME nº 05/2017.

8.3.4.24. Capacidade Técnica Operacional - devendo ser apresentada no ato de assinatura do contrato

8.3.4.24.1. Comprovação de possuir em seu quadro permanente, na condição de empregado (s) ou prestador (es) de serviço (s), as seguintes certificações:

8.3.4.24.2. Certificação Microsoft Certified Solutions Associate MCSA Windows Server 2012 no mínimo, para interação com o ambiente Microsoft;

Certificação de Firewall Sonicwall para interação com os produtos de segurança do CRCES;

8.3.4.24.3. Certificação para Instalação e Configuração de Switches DELL ou similar;

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de R\$40.000,00 (quarenta mil reais) perfazendo o valor total de R\$480.000,00 (quatrocentos e oitenta mil reais), apostos *tabela abaixo*:

ITEM 1					
SUBITEM	ESPECIFICAÇÃO	CATSER	QUANTIDADE	VALOR MENSAL	VALOR ANUAL
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	30710	12	R\$ 17.000,00	R\$ 204.000,00
2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	30736	12	R\$ 3.000,00	R\$ 36.000,00

3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	30728	12	R\$ 12.000,00	R\$ 144.000,00
4	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	30744	12	R\$ 8.000,00	R\$ 96.000,00

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES.

10.2. A contratação será atendida pela seguinte dotação:

· 6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

10.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação dos orçamentos pelo Conselho Federal de Contabilidade – CFC.

Vitória/ES, 21 de agosto de 2025.

Wekson José Barbieri Mariano

Operador de Sistemas

Aprovo o Termo de Referência.

Encaminhe-se para as providências necessárias para a seleção do fornecedor, cumprindo as demais etapas legais para a contratação pública.

Contador **Walterleno Maifrede Noronha**

Presidente



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 22/08/2025, às 07:48, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 25/08/2025, às 07:19, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

https://sei.cfc.org.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](#), informando o código verificador **0962132** e o código CRC **43C0DA56**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0962132

E-MAILS ENVIADOS

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:19
Para: 'comercial@ish.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:20
Para: 'print@printsolucao.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:18
Para: 'francisco@fdtecnologia.com'; 'franciscolaia@hotmail.com'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:18
Para: 'comercial@wedotec.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional: <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:19
Para: 'contato@mitrix.com.br'; 'comercial@mitrix.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:19
Para: 'comercial@admz.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:17
Para: 'vinicius@dtnetwork.com.br'; 'atendimento@dtnetwork.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:17
Para: 'contato@drtelecom.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: terça-feira, 12 de agosto de 2025 08:39
Para: 'ermelindo@redes.vix.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: segunda-feira, 11 de agosto de 2025 10:58
Para: 'camila.souza@tise.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: sexta-feira, 8 de agosto de 2025 11:32
Para: 'teixeira@wcompany.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: sexta-feira, 8 de agosto de 2025 11:31
Para: 'anderson.fernandes@clickti.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: sexta-feira, 8 de agosto de 2025 09:27
Para: 'contato@ayko.tech'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: sexta-feira, 8 de agosto de 2025 09:26
Para: 'paulo.pereira@luniobr.com'; 'ivanildo@luniobr.com'; 'danilo@luniobr.com'; 'ricardo.cardoso@luniobr.com'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica,	Mês	12

			gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: sexta-feira, 8 de agosto de 2025 09:24
Para: 'jeferson.guidoni@ayko.tech'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 10:02
Para: 'suporte@alterna.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:29
Para: 'comercial@admz.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:29
Para: 'eduardoms@mitrix.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:28
Para: 'wagner.perucci@terzian.com.br'; 'Amanda C'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional: <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:28
Para: Murilo Rupp; 'João Miguel Barcellos dos Santos'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:29
Para: 'flaviobatista@certa.inf.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:29
Para: 'leonardo@sc48.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:28
Para: 'Royce Santiago de Almeida'; Diego Carneiro
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:19
Para: 'moisesgrocha@mmitecnologia.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:16
Para: 'comercial-corporativo@alloha.com'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional: <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:17
Para: 'lpassos@verointernet.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:15
Para: 'otech@terzian.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:16
Para: 'AtendimentoAtacado@oi.net.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌱 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:16
Para: 'huawei.fsb@fsb.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:18
Para: 'atendimento@paestecnologia.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📧 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:18
Para: 'leonardo@sc48.com.br'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CRCES - Compras

De: CRCES - Compras
Enviado em: quinta-feira, 7 de agosto de 2025 09:16
Para: 'contato@certasolucoes.com'
Assunto: Orçamento - Gerenciamento de TI
Anexos: Termo de Referencia.pdf

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e	Mês	12

			mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.		
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**.

Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

📍 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



📍 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

🌿 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

E-MAILS
RECEBIDOS -
NEGATIVAS

CRCES - Compras

De: Natali Andrade <natali.andrade@wedotec.com.br>
Enviado em: quinta-feira, 7 de agosto de 2025 09:45
Para: CRCES - Compras; Comercial
Assunto: RES: Orçamento - Gerenciamento de TI

Olá bom dia !
CRCES - Compras compras@crc-es.org.br

Agradecemos o envio desse e-mail contudo sinalizamos que nossa empresa não atende ao escopo mencionado.

Atenciosamente,

Natáli A. Soares Baldson
Coordenadora da Administração de Vendas
+55 (27) 99275.7923



De: CRCES - Compras <compras@crc-es.org.br>
Enviada em: quinta-feira, 7 de agosto de 2025 09:23
Para: Comercial <comercial@wedotec.com.br>
Assunto: Orçamento - Gerenciamento de TI

Bom dia, prezados,

Solicito orçamento para contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos

links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, conforme tabela abaixo.

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01	30710	SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02	30736	FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04	30744	BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

Para **melhor compreensão** das demandas e especificações técnicas, encaminhamos em anexo o **Termo de Referência** da contratação.

Prazo para envio do orçamento: 03 (três) dias úteis a contar do recebimento deste e-mail.

Solicitamos que seja informado o CNPJ da empresa responsável pelo orçamento

O **CRCES** é reconhecido como um contratante responsável e comprometido com a boa administração pública, destacando-se pela transparência e eficiência em suas contratações. Nossas aquisições são realizadas por **dispensa de licitação ou pregão eletrônico**, por meio do portal oficial: www.gov.br/compras.

Para participação, é indispensável que a empresa esteja cadastrada previamente no portal de compras e no **Sistema de Cadastramento Unificado de Fornecedores – SICAF**. Os editais e avisos de contratação direta também são disponibilizados em nosso site institucional:

 <https://crc-es.org.br/novas-licitacoes>

Contamos com sua participação e aproveitamos para reforçar que o CRCES valoriza parcerias com fornecedores comprometidos com qualidade e responsabilidade.

Atenciosamente,



Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634

 Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

 Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece



PROPOSTAS RECEBIDAS

Proposta Comercial



clickTGroup

Soluções de Infraestrutura
& Serviços de TI

QUEM SOMOS

A Click TI Group é uma empresa de Campo Grande/MS com 14 anos de experiência no setor de tecnologia da informação para o mercado brasileiro. Nossa atuação se dá como **Provedora de Soluções e Serviços de TI**, e assim, fomentamos o desenvolvimento em ambientes de TI de alta disponibilidade, alta performance e segurança, de Instituições do Setor Público - nas esferas Municipal, Estadual e Federal - e Empresas do Setor Privado – SMB e Grande Porte.

A Click TI Group atua através da **Click TI Tecnologia** e da **Click TI Services**, sendo que cada uma delas tem um papel diferenciado:

A **Click TI Tecnologia** fica responsável por prover o avanço tecnológico através da venda de Soluções de Infraestrutura de TI (hardware e software), enquanto a **Click TI Services** fica responsável pela estruturação lógica, implementação e treinamentos da equipe do cliente, terceirização da TI, outsourcing de infraestrutura de TI, entre outros serviços personalizados que são de necessidade de cada perfil de cliente.

Belo Horizonte – MG, 13 de agosto de 2025.

Ao
CRC-ES
A/C: Maria Eduarda Storch

Proposta que faz a empresa CLICK TI TECNOLOGIA LTDA, inscrita no CNPJ 10.862.298/0004-45 e Inscrição Estadual nº 39.4629300-58, estabelecida na R. Maranhão 1694 – 2º andar, no bairro de Funcionários, na cidade de Belo Horizonte/MG.

Conforme solicitado, apresentamos a nossa proposta para o fornecimento de nossas Soluções e/ou Serviços de TI. No caso de eventuais dúvidas resultantes desta proposta, nos colocamos à sua disposição para esclarecimento das mesmas, através de telefone e/ou e-mail.

Agradecemos a oportunidade!

Anderson Fernandes

Anderson Fernandes

Diretor Comercial
☎ (31) 99715-6850
✉ anderson.fernandes@clickti.com.br

CONDIÇÕES COMERCIAIS

Para a aquisição das Soluções de Tecnologia/Serviços descritas, a **CRC-ES** deve estar ciente de que os valores que constam nesta Proposta Comercial prevalecem sob quaisquer outros termos e condições do Cliente, incluindo, mas não se limitando à Ordem de Compra emitida pelo Cliente.

Para um melhor entendimento, apresentamos abaixo o descritivo de valores para cada um dos itens entregáveis desta Proposta Comercial, bem como apresentamos o valor total de todas as Soluções de Tecnologia/Serviços.

ITEM	CASTER	DESCRIÇÃO COMPLEMENTAR	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	30710	DESCRIÇÃO: SOLUÇÃO DE ACESSO VIA WI-FI DESCRIÇÃO COMPLEMENTAR: Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12	R\$ 17.000,00	R\$ 204.000,00
2	30736	DESCRIÇÃO: FIREWALL (SEDE) DESCRIÇÃO COMPLEMENTAR:	Mês	12	R\$ 3.000,00	R\$ 36.000,00

		Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.				
3	30728	DESCRIÇÃO: SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3 DESCRIÇÃO COMPLEMENTAR: Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12	R\$ 12.000,00	R\$ 144.000,00
4	30744	DESCRIÇÃO: BACKUP CORPORATIVO DESCRIÇÃO COMPLEMENTAR: Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12	R\$ 8.000,00	R\$ 96.000,00
TOTAL						R\$ 480.000,00

FORMA DE PAGAMENTO

Integral em uma única parcela, até 30 (trinta) dias contados da data de recebimento da fatura

VALIDADE DA PROPOSTA

A presente proposta tem validade de 30 dias a partir de sua apresentação.

PRESTAÇÃO DE SERVIÇOS:

Os Serviços de TI serão prestados pela DELL na forma e dentro dos prazos definidos nos Objetivos & Entregas, se aplicável.

Atenção:

A entrega de Soluções de Tecnologia (produtos & equipamentos) adquiridos por Pessoa Jurídica/Instituições Públicas será realizado no endereço que consta registrado nos órgãos legais - Receita Federal e/ou Sintegra, não sendo possível a entrega em endereço divergente do que se encontra cadastrado.

FORNECEDOR & FATURAMENTO

Dados Faturamento:

FILIAL BELO HORIZONTE/MG

(Notas Fiscais de Mercadorias)

CLICK TI TECNOLOGIA LTDA.

R. Maranhão 1694, 2º andar – Bairro de Lourdes

Belo Horizonte/MG

CNPJ: 10.862.298/0004-45

I.E: 39.4629300-58

Atenção:

A NOTA FISCAL É EMITIDA DIRETO DO FORNECEDOR.

Caso haja diferença de ICMS ou qualquer tipo de imposto local, o pagamento/recolhimento do mesmo será de inteira responsabilidade do Cliente.

CONFIDENCIALIDADE

Ambas as partes envolvidas nesta Proposta Comercial devem considerar estritamente confidenciais todas as informações recebidas da outra parte, sejam essas informações relativas à negociação, incluindo, mas não se limitando as informações das Soluções de Tecnologia (produtos & equipamentos) /Serviços transmitidas em razão da presente proposta.

As partes comprometem-se à não transmitir nenhuma informação a terceiros, nem permitir que terceiros tomem conhecimento de tais informações, exceto quando em cumprimento a ordem de autoridades governamentais e/ou judiciais e no estrito cumprimento da lei.

Não serão consideradas confidencias aquelas informações que já forem de domínio público, notoriamente pertencentes à outra parte por razões comerciais anteriores ou exteriores a presente Proposta Comercial ou obtidas por fonte governamental.

A confidencialidade deverá ser respeitada pelo período de 5 anos, após o recebimento de qualquer informação confidencial.

Teresina-PI, 11 de agosto de 2025

AO**CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO**

Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620

Telefone: (27) 3232-1600 - www.crc-es.org.brE-mail: diretoria@crc-es.org.br

Att:

Prezada Maria Eduarda,

Apresentamos nossa proposta comercial conforme descrito abaixo, e planilha anexa:

OBJETO: Aquisição de serviços gerenciados de Tecnologia da Informação conforme condições, quantidades, exigências e estimativas estabelecidas neste instrumento.**REF.: PROCESSO:**

ITEM	DESCRIÇÃO	Und.	Qtd.	Unitário R\$	Total R\$
1	SOLUÇÃO DE ACESSO VIA WI-FI Demais configurações conforme solicitadas no Termo de Referência.	mês	12	R\$ 16.025,49	R\$ 192.305,88
2	FIREWALL (SEDE) Demais configurações conforme o termo de referência	mês	12	R\$ 3.271,89	R\$ 39.262,68
3	SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3 Demais configurações conforme o termo de referência	mês	12	R\$ 12.658,50	R\$ 151.902,00
4	BACKUP CORPORATIVO Demais configurações conforme solicitadas no Termo de Referência.	mês	12	R\$ 9.881,00	R\$ 118.572,00
	TOTAL DA PROPOSTA			R\$ 41.836,88	R\$ 502.042,56

CONDIÇÕES COMERCIAIS	
Cond. de Pagto	A vista em até 10 dias da apresentação da nota fiscal.
Validade da Proposta	60 dias.
Prazo de Entrega	Conforme contrato e recebimento do empenho.
Faturamento	Faturamento em Teresina-Pi
Moeda	R\$ (Reais)
Frete	Inclusos
Impostos	Inclusos Nos valores dos itens deverão estar inclusos todos os custos, passagens, diárias, impostos, taxas, seguros, fretes, riscos, materiais de consumo, peças, produtos e mão de obra, necessários ao bom desempenho dos serviços.
DADOS P/ ASSINATURA DO CONTRATO	Razão Social: FORTECOM LTDA CNPJ.: 01.559.646/0001-76 I.E.: 19.451.608-3 I. MUNIC.: 072064-0 Av. Fernando Pires Leal, 2000 / Sala-04 – São João Teresina - PI CEP: 64.045-550 Fone: 86 3301-5378/5350 98823-1314 E-Mail: teixeira@wcompany.com.br

FORTECOM LTDA CNPJ (MF): 01.559.646/0001-76 Insc. Estadual: 19.451.608-3 CMC: 072064-0

Av. Fernando Pires Leal, 2000 / Sala-04 – São João Teresina - PI CEP: 64.045-550

Tel.: 86 3301-5350 / **9 8823-1314** E-mail: teixeira@wcompany.com.br **Pág.: 1/2**

Atenciosamente,



Antônio das Neves do N. **TEIXEIRA**
Depto Contas Corporativas e Governos
Fone: 86 3301-5350 / 98823-1314
Email: teixeira@wcompany.com.br



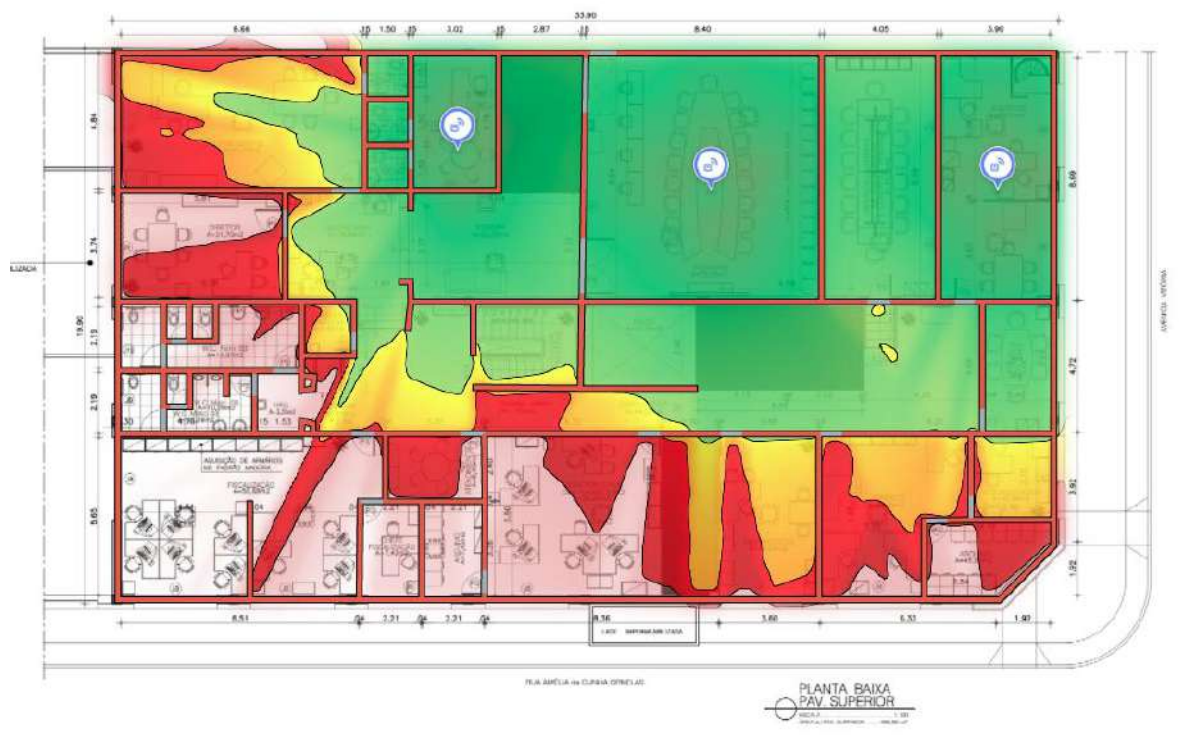
À(o) Conselho Regional Contabilidade do Espírito Santo - CRCES

Apresentamos nossa Proposta Comercial para fornecimento de equipamentos de informática, conforme a descrição abaixo:

ITEM	DESCRIÇÃO	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01	Marca: Fortinet Modelo: FAP-231G-N + FS-124F-POE Descrição resumida: SOLUÇÃO DE ACESSO VIA WI-FI Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES Descrições conforme o Termo de Referência.	12	R\$ 17.552,06	R\$ 210.624,72
02	Marca: Fortinet Modelo: Fortigate-80F Descrição resumida: SOLUÇÃO DE FIREWALL (SEDE) Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas. Descrições conforme o Termo de Referência.	12	R\$ 3.338,67	R\$ 40.064,04
03	Marca: PRINT Descrição resumida: SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3 Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI. Descrições conforme o Termo de Referência.	12	R\$ 13.050,00	R\$ 156.600,00
04	Marca: PRINT Descrição resumida: BACKUP CORPORATIVO Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD. Descrições conforme o Termo de Referência.	12	R\$ 11.700,00	R\$ 140.400,00
TOTAL			R\$ 45.640,73	R\$ 547.688,76

Plantas utilizadas para o dimensionamento da solução:

1. Planta baixa pav. Superior 1:



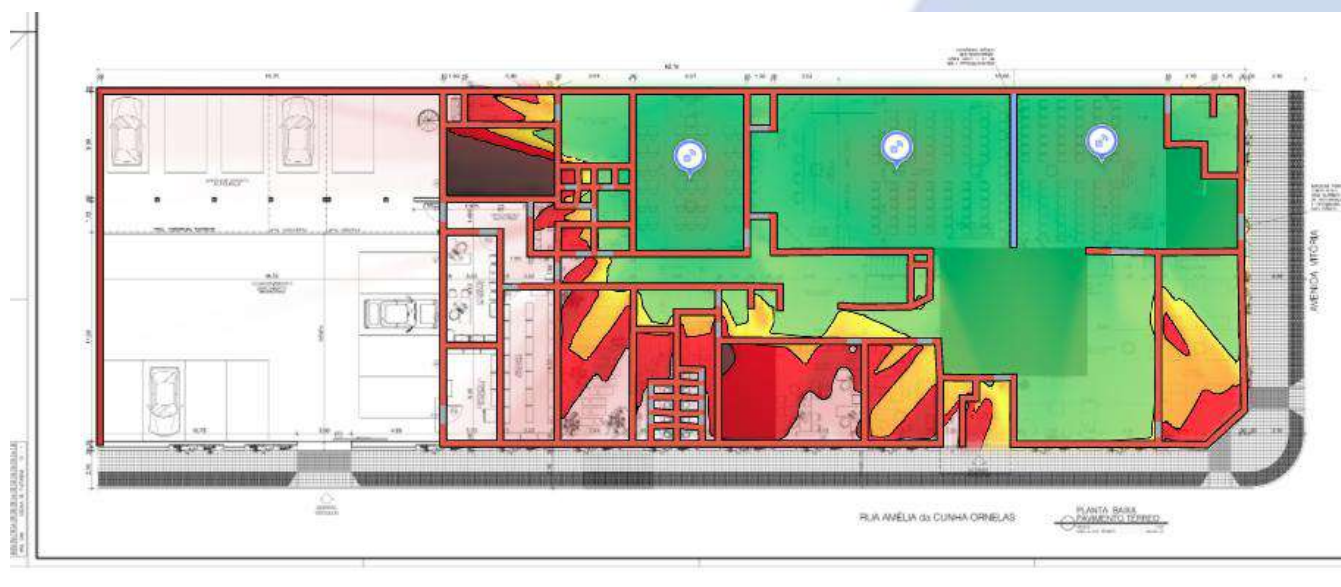
1.2 Planta baixa pav. Superior 2:



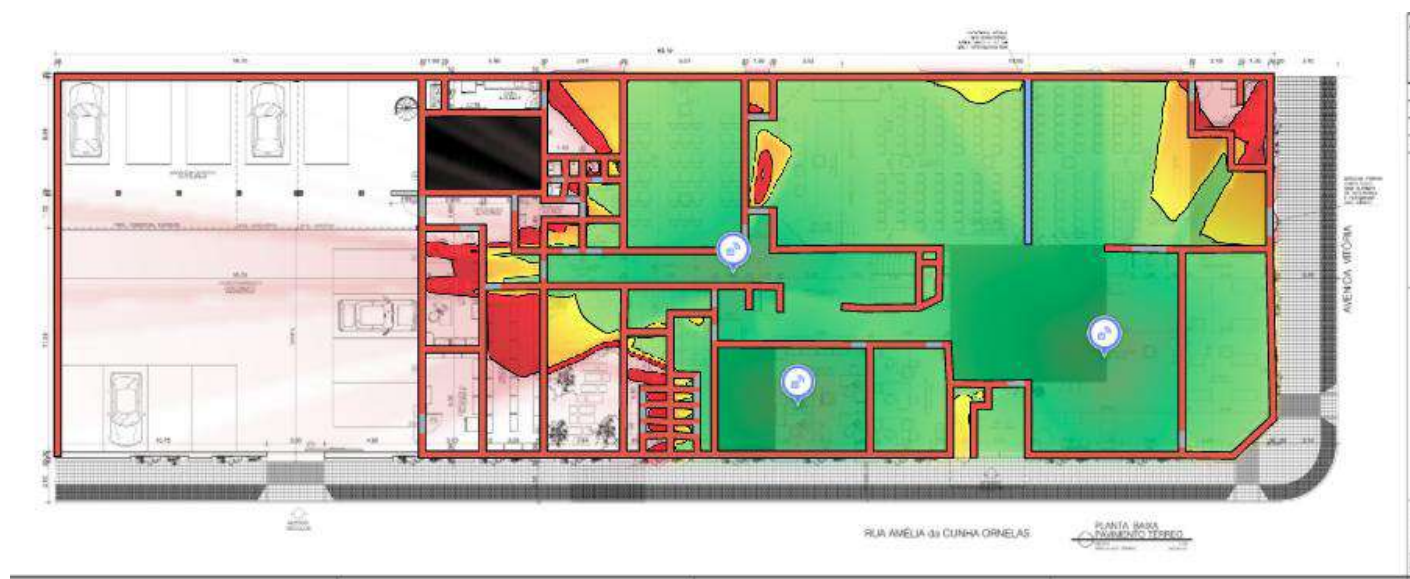
1.3 Planta baixa pav. Superior 3:



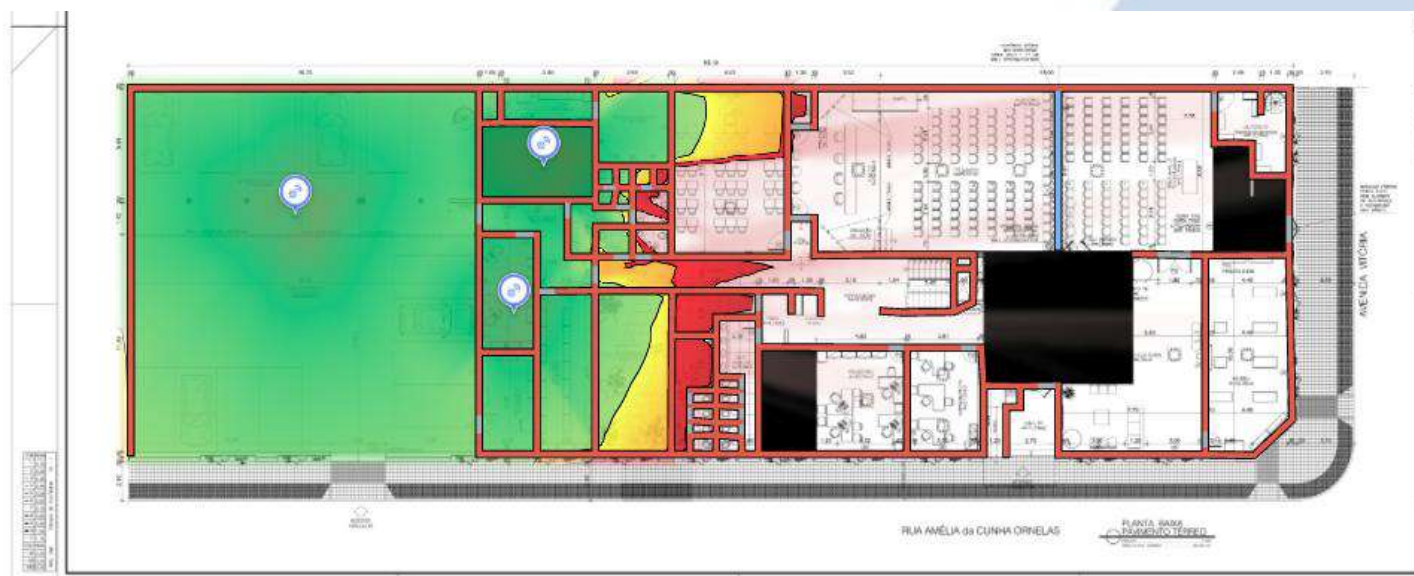
2. Planta baixa pav. Térreo 1:



2.2 Planta baixa pav. Térreo 2:



2.3 Planta baixa pav. Térreo 3:



Validade da Proposta: 60 dias.

Prazo de Entrega: 30 dias.

Em nossos preços unitários estão incluídos todos os custos diretos e indiretos para o perfeito fornecimento dos itens, inclusive das despesas com frete ou dispêndios resultantes de impostos Estaduais e Federais, e tudo o que for necessário para o fornecimento total e completo do item, bem como nosso lucro, sem que nos caiba, em qualquer caso, direito regressivo em relação à(o) **Conselho Regional Contabilidade do Espírito Santo – CRCES**.

Dados da Empresa:

Razão Social: PRINT SOLUÇÃO EM TECNOLOGIA LTDA

CNPJ: 15.549.061/0001-80

Inscrição Estadual: 08.287.465-4

Inscrição Municipal: 53673-0

Endereço: Rua Maranhão, nº 575, Salas 501, 502, 503 e 504 – Praia da Costa – Vila Velha/ES – CEP: 29.101-340

Dados Bancário: Banco [REDACTED]

E-mail: print@printsolucao.com.br

Vila Velha, 8 de agosto de 2025.

Atenciosamente,

A handwritten signature in black ink, appearing to read "Walter Maia Rodrigues Junior".

Walter Maia Rodrigues Junior
Diretor Comercial

PNCP
PORTAL NACIONAL DE
CONTRATAÇÕES
PÚBLICAS

Contratações

Consulte os [contratos públicos](#) e outros instrumentos hábeis substitutivos.

Palavra-chave

Fornecimento, instalação e gestão de rede Wi-Fi completa

Status

- ☐ Vigentes
- ☐ Não vigentes
- ☒ Todos

FILTROS



Tipos de Instrumento Convocatório

Selecione

Tipos de contrato

Selecione

Órgãos

Selecione

Unidades

Selecione

UFs

Selecione

Municípios

Selecione

Esferas

Selecione

Poderes

Selecione

Limpar

 Pesquisar

Nenhum resultado encontrado para "Fornecimento, instalação e gestão de rede Wi-Fi completa"

Sugestões:

- Certifique-se de que o termo foi digitado corretamente
- Tente outra palavra-chave
- Tente palavras-chave mais gerais

 Voltar



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.



É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correteza das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portaldeservicos.gestao.gov.br>

☎ 0800 978 9001

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à **licença de uso**.

Consulte os [contratos públicos](#) e outros instrumentos hábeis substitutivos.

Palavra-chave

Instalação e gestão de Firewall de próxima geração

Status

- ☐ Vigentes
- ☐ Não vigentes
- ☒ Todos

 FILTROS



Tipos de Instrumento Convocatório

Selecione

Tipos de contrato

Selecione

Órgãos

Selecione

Unidades

Selecione

UFs

Selecione

Municípios

Selecione

Esferas

Selecione

Poderes

Selecione

Limpar

 Pesquisar

Nenhum resultado encontrado para "Instalação e gestão de Firewall de próxima geração "

Sugestões:

- Certifique-se de que o termo foi digitado corretamente
- Tente outra palavra-chave
- Tente palavras-chave mais gerais

 Voltar



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.



É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correteza das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portaldeservicos.gestao.gov.br>

☎ 0800 978 9001

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à **licença de uso**.

Contratações

Editais e Avisos de Contratações

Atas de Registro de Preços

Contratos

Consulte os [contratos públicos](#) e outros instrumentos hábeis substitutivos.

Palavra-chave

Suporte técnico avançado para manutenção da infraestrutura tecnológica

Status

- ☒ Vigentes
☐ Não vigentes
☐ Todos

FILTROS



Tipos de Instrumento Convocatório

Selecione

Tipos de contrato

Selecione

Órgãos

Selecione

Unidades

Selecione

UFs

Selecione

Municípios

Selecione

Esferas

Selecione

Poderes

Selecione

Limpar

Pesquisar

Contratos Vigentes

Termo Pesquisado: Suporte técnico avançado para manutenção da infraestrutura tecnológica

Exibindo: 2 de 2

Ordenar por: Mais recente

Contrato nº 91146/2024

Última Atualização: 10/01/2025

Id contrato PNCP: 00038166000105-2-000373/2024

Modalidade da Contratação: Pregão - Eletrônico Última Atualização: 10/01/2025

Órgão: BANCO CENTRAL DO BRASIL Local: Brasília/DF Vigência: de 02/01/2025 a 02/01/2028

Objeto: CONTRATAÇÃO DE CESSÃO TEMPORÁRIA DE LICENÇAS, GARANTIA E SUPORTE TÉCNICO AVANÇADO DO SOFTWARE SPLUNK ENTERPRISE; SERVIÇOS PROFISSIONAIS ESPECIALIZADOS DA SPLUNK E SERVIÇOS DE MANUTENÇÃO DA INFRAESTRUTURA SPLUNK DO BANCO CENTRAL.

Valor Global Contratado: R\$ 843.085,05

Contrato nº 0157/24/2024

Última Atualização: 19/11/2024

Id contrato PNCP: 00877406000157-2-000085/2024

Modalidade da Contratação: Dispensa Última Atualização: 19/11/2024

Órgão: CONSORCIO INTERMUNICIPAL DE SAUDE UNIAO DA MATA Local: Leopoldina/MG Vigência: de 18/11/2024 a 17/11/2025

Objeto: Contratação de empresa especializada em Tecnologia da Informação para o fornecimento e gestão de ativos de infraestrutura na modalidade Hardware as a Service (HaaS), abrangendo a instalação, manutenção proativa e reativa, documentação técnica detalhada e serviços de suporte técnico especializado de nível 3 para toda a infraestrutura de data center, tanto para as instalações a serem implementadas quanto para as já existentes. O serviço deve atender integralmente às exigências de segurança da info ...

Valor Global Contratado: R\$ 68.800,00

1-2 de 2 itens

1

10



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.

É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correitude das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

 <https://portaldeservicos.gestao.gov.br>

 0800 978 9001

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à licença de uso.

Consulte os [contratos públicos](#) e outros instrumentos hábeis substitutivos.

Palavra-chave

Implementação e gestão de solução de backup local e em nuvem

Status

- ☒ Vigentes
☐ Não vigentes
☐ Todos

 FILTROS



Tipos de Instrumento Convocatório

Selecione

Tipos de contrato

Selecione

Órgãos

Selecione

Unidades

Selecione

UFs

Selecione

Municípios

Selecione

Esferas

Selecione

Poderes

Selecione

Limpar

 Pesquisar

Nenhum resultado encontrado para "Implementação e gestão de solução de backup local e em nuvem"

Sugestões:

- Certifique-se de que o termo foi digitado corretamente
- Tente outra palavra-chave
- Tente palavras-chave mais gerais

 Voltar



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.



É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correteza das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portaldeservicos.gestao.gov.br>

☎ 0800 978 9001

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à **licença de uso**.

PAINEL DE PREÇOS

MÉDIA

R\$

751.594,45

MEDIANA

R\$

745.028,50

MENOR

R\$

637.320,80

Quantidade total de registros: 4

Registros apresentados: 1 a 4

FILTROS APLICADOS

Objeto da Compra

9 of 72264

Modalidade da Compra

Pregão, Dispensa de Licitação

Esfera

Federal, Estadual, Municipal

RESULTADO 1

DADOS DA COMPRA

Identificação da Compra: 90027/2025

Número do Item: 00003

Objeto da Compra: Pregão Eletrônico - Contratação de empresa especializada no fornecimento, implementação e repasse de conhecimento de solução de plataforma de nuvem privada, composta por hardware e software, Plataforma de nuvem privada com processamento gráfico e cálculo aritmético, composta por hardware e software, solução de backup, composta pela renovação do contrato de suporte do atual software de backup e fornecimento de equipamento para armazenamento dos dados de backup e solução para armazenamento da

Quantidade Ofertada: 4

Valor Proposto Unitário: -

Valor Unitário do Item: R\$ 637320,8

Código do CATMAT: 25917

Descrição do Item: DESENVOLVIMENTO E/OU EVOLUCAO DE SOFTWARE - OUTRAS LINGUAGENS

Descrição Complementar:

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Modalidade da Compra: Pregão

Forma de Compra: SISRP

Marca:

Data do Resultado: 08/05/2025

DADOS DO FORNECEDOR

Nome do Fornecedor: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

CNPJ/CPF: 02092332000330

Porte do Fornecedor: Outros

DADOS DO ÓRGÃO

Número da UASG: 927996 - EAC-SECRETARIA DE EST.INDÚST.CIÊNCIA E TECNOL

Órgão: EAC-SECRETARIA DE EST.INDÚST.CIÊNCIA E TECNOL

Órgão Superior: -

RESULTADO 2

DADOS DA COMPRA

Identificação da Compra: 90011/2024

Número do Item: 00001

Objeto da Compra: Pregão Eletrônico - Aquisição de solução de conectividade sem fio (Wi-Fi) à rede corporativa, composta por pontos de acesso, controladoras e switches de acesso, com garantia e suporte oficial do fabricante por 60 (sessenta) meses, incluindo serviços de instalação, configuração e manutenção preventiva, corretiva e evolutiva.

Quantidade Ofertada: 1

Valor Proposto Unitário: -

Valor Unitário do Item: R\$ 641057

Código do CATMAT: 27464

Descrição do Item: LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR

Descrição Complementar:

Unidade de Fornecimento: UNIDADE

Modalidade da Compra: Pregão

Forma de Compra: SISPP

Marca:

Data do Resultado: 26/07/2024

DADOS DO FORNECEDOR

Nome do Fornecedor: LETTEL DISTRIBUIDORA DE TELEFONIA LTDA

CNPJ/CPF: 07789113000167

Porte do Fornecedor: Outros

DADOS DO ÓRGÃO

Número da UASG: 110404 - DEPARTAMENTO DE ADMINISTRAÇÃO INTERNA

Órgão: MINISTERIO DEFESA

Órgão Superior: PRESIDENCIA DA REPUBLICA - PRES

RESULTADO 3

DADOS DA COMPRA

Identificação da Compra: 90075/2024

Número do Item: 00001

Objeto da Compra: Pregão Eletrônico - Contratação de empresa especializada em serviços de suporte de nível 3 (N3) e nível 4 (N4) em TI, com foco em redes e servidores, para fornecer suporte técnico de alta qualidade, resolução de problemas avançados, manutenção proativa e assistência em projetos de infraestrutura de tecnologia da informação, CONFORME EDITAL E ANEXOS.

Quantidade Ofertada: 1

Valor Proposto Unitário: -

Valor Unitário do Item: R\$ 849000

Código do CATMAT: 27014

Descrição do Item: SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DAINFORMACAO E COMUNICACAO (TIC)

Descrição Complementar:

Unidade de Fornecimento: UNIDADE

Modalidade da Compra: Pregão

Forma de Compra: SISPP

Marca:

Data do Resultado: 19/11/2024

DADOS DO FORNECEDOR

Nome do Fornecedor: IT-ONE TECNOLOGIA DA INFORMACAO S.A.

CNPJ/CPF: 05333907000781

Porte do Fornecedor: Outros

DADOS DO ÓRGÃO

Número da UASG: 926483 - SERVICO SOCIAL DO COMERCIO - SESC AR/MG

Órgão: SERVICO SOCIAL DO COMERCIO - SESC AR/MG

Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL

RESULTADO 4

DADOS DA COMPRA

Identificação da Compra: 90027/2025

Número do Item: 00011

Objeto da Compra: Pregão Eletrônico - Contratação de empresa especializada no fornecimento, implementação e repasse de conhecimento de solução de plataforma de nuvem privada, composta por hardware e software, Plataforma de nuvem privada com processamento gráfico e cálculo aritmético, composta por hardware e software, solução de backup, composta pela renovação do contrato de suporte do atual software de backup e fornecimento de equipamento para armazenamento dos dados de backup e solução para armazenamento da

Quantidade Ofertada: 4

Valor Proposto Unitário: -

Valor Unitário do Item: R\$ 879000

Código do CATMAT: 27090

Descrição do Item: OUTROS SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)

Descrição Complementar:

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Modalidade da Compra: Pregão

Forma de Compra: SISRP

Marca:

Data do Resultado: 08/05/2025

DADOS DO FORNECEDOR

Nome do Fornecedor: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

CNPJ/CPF: 02092332000330

Porte do Fornecedor: Outros

DADOS DO ÓRGÃO

Número da UASG: 927996 - EAC-SECRETARIA DE EST.INDÚST.CIÊNCIA E TECNOL

Órgão: EAC-SECRETARIA DE EST.INDÚST.CIÊNCIA E TECNOL

Órgão Superior: -

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

MAPA DE COMPARATIVO DE PREÇOS

Conforme diretrizes da Instrução Normativa nº 65/2021.

Objeto: Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

FORNECEDORES

CLICK TI TECNOLOGIA LTDA

FORTECOM LTDA

**PRINT SOLUÇÃO EM
TECNOLOGIA LTDA**

CNPJ: 10.862.298/0004-45

CNPJ: 01.559.646/0001-76

CNPJ: 15.549.061/0001-80

Itens	Descrição	Qnt	Valor Mensal	Valor Anual	Valor Mensal	Valor Anual	Valor Mensal	Valor Anual
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	12	R\$ 17.000,00	R\$ 204.000,00	R\$ 16.025,49	R\$ 192.305,88	R\$ 17.552,06	R\$ 210.624,72

2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	12	R\$ 3.000,00	R\$ 36.000,00	R\$ 3.271,89	R\$ 39.262,68	R\$ 3.338,67	R\$ 40.064,04
3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	12	R\$ 12.000,00	R\$ 144.000,00	R\$ 12.658,50	R\$ 151.902,00	R\$ 13.050,00	R\$ 156.600,00

4	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	12	R\$ 8.000,00	R\$ 96.000,00	R\$ 9.881,00	R\$ 118.572,00	R\$ 11.700,00	R\$ 140.400,00
				R\$ 480.000,00			R\$ 502.042,56	R\$ 547.688,76



Documento assinado eletronicamente por **Maria Eduarda Storch Magalhães, Assessora**, em 15/08/2025, às 09:06, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0974303** e o código CRC **E0B93195**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

A pesquisa de preços destinada à determinação do valor estimado para o objeto deste Mapa Comparativo de Preços foi conduzida em conformidade com os parâmetros estabelecidos na Instrução Normativa SEGES/ME nº 65/2021 e no artigo 23, §1º, incisos II e IV, da Lei Federal nº 14.133/2021, que preveem, respectivamente:

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

Para a elaboração da presente pesquisa, adotaram-se os seguintes parâmetros:

Pesquisa direta junto a fornecedores, mediante solicitação formal de cotação;

Consulta a sistemas oficiais, notadamente o *Painel Nacional de Contratações Públicas* (PNCP) e o *Painel de Preços* do Governo Federal.

Conforme demonstrado na peça nº 0974302, a consulta ao Painel de Preços teve como objetivo ampliar a base de referências para análise comparativa, resultando na identificação de 04 (quatro) processos, porém nenhum deles podem se considerados similares.

Para esta filtragem, foram utilizados os seguintes parâmetros:

Esfera: Todos;

Modalidade: Pregão e Dispensa de Licitação;

Descrição do item: “Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa”, “Instalação e gestão de Firewall de Próxima Geração”, “Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica” e “Implementação e gestão de solução de backup local e em nuvem”.

Além disso, foi realizada pesquisa detalhada pelo Portal Nacional de Contratações Públicas (PNCP), mas também não foram localizados contratos que pudessem ser considerados similares, reforçando a necessidade de se fundamentar a análise principalmente nas propostas coletadas diretamente junto aos fornecedores.

Foram encaminhadas solicitações de cotação a trinta e duas (32) empresas, das quais apenas uma (01) respondeu negativamente e três (03) apresentaram propostas que compõem o Mapa Comparativo de Preços, constante da peça nº 0974303. Sendo elas:

- Click TI Tecnologia Ltda;

- Fortecom Ltda;
- Print Solução em Tecnologia Ltda.

A seleção dos fornecedores foi baseada em levantamento prévio de mercado, considerando empresas com atuação comprovada, mediante consultas a registros comerciais, bases públicas e cadastros de fornecedores já homologados.

Em cumprimento ao disposto no art. 6º, §4º, da Instrução Normativa SEGES/ME n.º 65/2021;

§ 4º *Os preços coletados devem ser analisados de forma crítica, em especial, quando houver grande variação entre os valores apresentados.*

Assim, todas as propostas recebidas foram analisadas de forma crítica, considerando aspectos como a compatibilidade técnica dos produtos ofertados, a regularidade fiscal das empresas, a reputação dos fornecedores no mercado e a coerência dos valores apresentados em relação aos parâmetros praticados no setor. Essa análise criteriosa teve como objetivo assegurar que os preços utilizados na estimativa fossem representativos da realidade de mercado e compatíveis com a qualidade e as especificações exigidas.

Dessa forma, foram mantidas na análise final as seguintes referências, por apresentarem maior grau de compatibilidade entre si:

- Click TI Tecnologia Ltda: R\$ 480.000,00 (quatrocentos e oitenta mil reais);
- Fortecom Ltda: R\$ 502.042,56 (quinhentos e dois mil quarenta e dois reais e cinquenta e seis centavos);
- Print Solução em Tecnologia Ltda: R\$ 547.688,76 (quinhentos e quarenta e sete mil seiscentos e oitenta e oito reais e setenta e seis centavos).

Considerando a metodologia de avaliação adotada, a definição do valor de referência e a comparação entre as propostas foram pautadas pelo menor preço apurado dentre as cotações consideradas válidas. Tal critério foi estabelecido em estrita observância ao princípio da economicidade, com o propósito de assegurar que a Administração obtenha a solução mais vantajosa sob o ponto de vista financeiro, sem que isso implique em qualquer prejuízo à qualidade ou à conformidade técnica dos serviços e produtos a serem contratados.

A adoção do menor valor como parâmetro de referência permite uma análise consistente, objetiva e transparente, fortalecendo a racionalidade na condução do processo licitatório e contribuindo significativamente para a mitigação do risco de sobrepreço. Além disso, tal metodologia promove a segurança jurídica e a previsibilidade das decisões, em alinhamento com as melhores práticas de gestão pública.

Diante disso, foi fixado como preço de referência o montante de R\$ 480.000,00 (quatrocentos e oitenta mil reais), valor que servirá de base para a análise de compatibilidade da proposta vencedora com os preços praticados no mercado, garantindo que a contratação seja realizada em condições justas e vantajosas para a Administração.

Diante do exposto, conclui-se que a pesquisa de preços foi conduzida de maneira técnica, criteriosa e fundamentada, atendendo integralmente às disposições legais e normativas vigentes. Todos os procedimentos adotados asseguraram a adequada formação do preço de referência, refletindo valores compatíveis com o mercado e proporcionando à Administração condições de contratar de forma eficiente, econômica e transparente, resguardando o interesse público e garantindo a legalidade do processo.



Documento assinado eletronicamente por **Maria Eduarda Storch Magalhães, Assessora**, em 15/08/2025, às 09:01, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0974305** e o código CRC **B96924EB**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0974305

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

JUSTIFICATIVA PARA AUSÊNCIA DE RESERVA ORÇAMENTÁRIA PRÉVIA

(Processo relativo à contratação de serviços gerenciados de Tecnologia da Informação)

Nos termos do artigo 7º do Decreto nº 10.540/2020, que estabelece os parâmetros mínimos para um sistema de administração financeira e controle, e em conformidade com os princípios da legalidade, economicidade, eficiência, continuidade do serviço público e planejamento, apresento a justificativa para a ausência de reserva orçamentária prévia no procedimento licitatório em curso relativo à **contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.**

O objeto da contratação contempla o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa contratada será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo inclui suporte técnico remoto e presencial para uma localidade, atendimento a até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais, além da gestão e manutenção do banco de dados em SQL Server, manutenção preventiva e corretiva de todo o parque de TI, gestão e monitoramento dos links de internet e gestão da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas no instrumento contratual.

A ausência de reserva orçamentária prévia se justifica pelos seguintes fundamentos:

- **Vigência contratual atual assegurada:** a infraestrutura tecnológica crítica para as operações do CRCES permanece operante, garantindo a continuidade dos serviços até 31 de janeiro de 2026;
- **Execução condicionada ao novo exercício:** a nova contratação será executada a partir de fevereiro de 2026, vinculando-se integralmente ao orçamento do exercício seguinte;
- **Planejamento em andamento:** a despesa já está considerada no planejamento orçamentário institucional em elaboração, cujo Plano de Trabalho será consolidado até setembro de 2025, conforme cronograma oficial;
- **Previsão de empenho futuro:** os valores referentes à contratação serão regularmente empenhados dentro do orçamento de 2026, em observância aos princípios da responsabilidade fiscal.

Cabe destacar que a postergação da fase interna do procedimento licitatório até a aprovação do orçamento de 2026 comprometeria o cronograma necessário para a conclusão regular do certame, trazendo risco de descontinuidade na prestação dos serviços de TI essenciais. Tal cenário impactaria diretamente o funcionamento do CRCES, prejudicando a execução das atividades administrativas e técnicas e comprometendo a continuidade das operações da instituição.

Portanto, a tramitação do processo licitatório até as fases de julgamento, homologação e assinatura

contratual se mostra plenamente justificável, não havendo óbice legal à sua continuidade, desde que a execução financeira ocorra exclusivamente após o início da vigência do novo contrato e dentro dos limites fixados pela Lei Orçamentária Anual de 2026.



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 21/08/2025, às 17:58, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0985529** e o código CRC **A93137D1**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0985529

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

JUSTIFICATIVA E APROVAÇÃO DO PROCESSO LICITATÓRIO

Trata-se da **contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação** para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES.

O objeto contempla o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa contratada será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores.

O escopo inclui suporte técnico remoto e presencial para uma localidade, atendimento a até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais, além da gestão e manutenção do banco de dados em SQL Server, manutenção preventiva e corretiva de todo o parque de TI, gestão e monitoramento dos links de internet e gestão da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.

Até o momento, integram o processo os seguintes documentos:

- Documento de Formalização de Demanda;
- Portaria nº 042/2024, que nomeia os membros das equipes de planejamento das contratações do CRCES;
- Estudo Técnico Preliminar;
- Mapa de Riscos do planejamento da contratação;
- Termo de Referência;
- Mapa de Riscos da seleção do fornecedor;
- Pesquisa de preços de mercado e mapa comparativo de preços;
- Despacho de solicitação de reserva orçamentária.

Diante da essencialidade do serviço, justifica-se a necessidade de contratação ininterrupta, garantindo a continuidade das atividades do CRCES, a modernização da infraestrutura tecnológica e a plena execução de suas funções institucionais. Trata-se de solução indispensável, cuja interrupção comprometeria diretamente a produtividade dos colaboradores e, por consequência, a eficiência administrativa da autarquia.

Ressalta-se que a contratação poderá se estender por mais de um exercício financeiro, uma vez que a manutenção e gestão da infraestrutura de TI é imprescindível para a execução contínua das atividades do CRCES. A prestação dos serviços assegura condições adequadas de operação, segurança, comunicação e produtividade, em conformidade com os padrões tecnológicos adotados pela Administração Pública.

Diante da relevância do serviço, a contratação torna-se imprescindível, representando uma medida

estratégica para a modernização tecnológica, a continuidade e a eficiência das operações do CRCES.

Considerando que toda a documentação necessária à formalização do processo já foi devidamente reunida, **APROVO** a abertura do Processo Licitatório, na modalidade **Pregão Eletrônico**, e **AUTORIZO** o envio do processo ao pregoeiro para a devida tramitação, com o cumprimento das formalidades legais necessárias à seleção do fornecedor.



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 25/08/2025, às 07:18, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0985548** e o código CRC **CE6D2D69**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0985548



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

MINUTA DE CONTRATO

Processo nº 9079618110000798.000048/2025-57

Contrato DE [DIGITE AQUI O OBJETO] QUE
CELEBRAM ENTRE SI A CONSELHO REGIONAL
DE CONTABILIDADE DO ESPÍRITO SANTO E A
[DIGITE AQUI O NOME DA EMPRESA].

O CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO – CRCES, Autarquia Federal de Regime Especial, inscrito no CNPJ – sob o n.º 28.163.343/0001-96, com sede à Rua Amélia da Cunha Ornelas, nº 30, Bento Ferreira, Vitória/ES, CEP: 29.050- 620, representado pelo seu Presidente, o Contador WALTERLENO MAIFREDE NORONHA, nomeado pela Ata nº 1.664, de 02 de janeiro de 2024, doravante denominado CONTRATANTE, e o(a), inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, em doravante designado CONTRATADO, neste ato representado(a) por (nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº 9079618110000798.000048/2025-57 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. xx/202X, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO ([art. 92, I e II](#))

1.1. O objeto do presente instrumento é contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.

TEM 1			
SUBITEM	ESPECIFICAÇÃO	CATSER	QUANTIDADE
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	30710	12
2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	30736	12
3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	30728	12
4	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	30744	12

1.2. Vinculam esta contratação, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. O Aviso de Contratação;

1.2.3. A Proposta do contratado;

1.2.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

- c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;
- d) Haja manifestação expressa do contratado informando o interesse na prorrogação;
- e) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS ([art. 92, IV, VII e XVIII](#))

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA – PREÇO ([art. 92, V](#))

5.1. O valor mensal estimado da contratação é de R\$ (.....), perfazendo o valor total estimado de R\$ (.....).

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA – CRITÉRIOS DE PAGAMENTO E MEDIÇÃO ([art. 92, V e VI](#))

6.1 O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

6.2 No caso de atraso de pagamento(s) pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente pelo índice IPCA - Índice de Preços ao Consumidor Amplo, bem como incidirão juros moratórios, à razão de 0,5% (meio por cento) ao mês, aplicando-se a fórmula constante em item 5 do Anexo XI da Instrução Normativa nº 05, de 26 de maio de 2017.

7. CLÁUSULA SÉTIMA - REAJUSTE ([art. 92, V](#))

7.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, em 26/05/2025.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IPCA - Índice de Preços ao Consumidor Amplo (acumulado nos últimos 12 meses desde a apresentação da proposta), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos

efeitos financeiros do último reajuste.

7.4. No caso de atraso ou não divulgação do índice de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

7.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

7.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE ([art. 92, X, XI e XIV](#))

8.1. São obrigações do Contratante:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9. Cientificar o Setor Jurídico do CRCES para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.10.1. A Administração terá o prazo de 05 (cinco) dias úteis, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.11. Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro, bem como de repactuação de preços, feitos pelo contratado no prazo máximo de 30 dias.

8.13. Comunicar ao Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.15. Demais obrigações descritas no Termo de Referência.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO ([art. 92, XIV, XVI e XVII](#))

- 9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:
- 9.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior ([art. 137, II](#)) e prestar todo esclarecimento ou informação por eles solicitados;
- 9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 9.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o [Código de Defesa do Consumidor \(Lei nº 8.078, de 1990\)](#) , bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;
- 9.5. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do [artigo 48, parágrafo único, da Lei nº 14.133, de 2021](#) ;
- 9.6. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, bem como aos documentos relativos à execução do objeto.
- 9.7. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 9.8. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças na execução do objeto.
- 9.9. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 9.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- 9.11. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116](#));
- 9.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único](#));
- 9.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 9.14. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no [art. 124, II, d, da Lei nº 14.133, de 2021](#);
- 9.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;
- 9.16. Demais obrigações descritas no Termo de Referência.

10. CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a [Lei nº 13.709, de 14 de agosto de 2018 \(LGPD\)](#) , quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de

contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do [art. 6º da LGPD](#).

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do [art. 15 da LGPD](#), é dever do contratado eliminá-los, com exceção das hipóteses do [art. 16 da LGPD](#), incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados ([LGPD, art. 37](#)), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.12. Os contratos e convênios de que trata o [§ 1º do art. 26 da LGPD](#) deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO ([art. 92, XII](#))

11.1. Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS ([art. 92, XIV](#))

12.1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2 Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

12.3 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

12.4 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

12.5 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

12.6 Multa:

12.6.1 Moratória, para as infrações descritas no item “d”, de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (sessenta) dias [\[A1\]](#) [\[A2\]](#) , observados os limites previstos no §3º do art. 156.

12.6.2 Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia; [\[A3\]](#)

12.6.3 O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

12.6.4 Compensatória, para as infrações descritas acima nas alíneas “e” a “h” de 0,5% (cinco décimos por cento) a [\[A4\]](#) 30% (trinta por cento) do valor da contratação.

12.6.5 Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.6 Compensatória, para a infração descrita acima na alínea “b”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.7 Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.8 Compensatória, para a infração descrita acima na alínea “a”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.9 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

12.6.10 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

12.6.11 Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.6.12 Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

12.6.13 A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.6.14 A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art.

158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6.15 Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

12.6.16 Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicafe serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

12.6.17 Na aplicação das sanções serão considerados os elementos previstos no §1º do art. 156.

12.6.18 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

12.6.19 A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

12.6.20 O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

12.6.21 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

12.6.22 Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL ([art. 92, XIX](#))

13.1. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/21](#), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.1.1. Nesta hipótese, aplicam-se também os [artigos 138 e 139](#) da mesma Lei.

13.1.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.1.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.2. O termo de extinção, sempre que possível, será precedido:

13.2.1.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.2.1.2. Relação dos pagamentos já efetuados e ainda devidos;

13.2.1.3. Indenizações e multas.

13.3. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-

financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131, caput, da Lei n.º 14.133, de 2021](#)).

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA ([art. 92, VIII](#))

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES, na dotação abaixo discriminada:

6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS ([art. 92, III](#))

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na [Lei nº 14.133, de 2021](#), e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

18. CLÁUSULA DÉCIMA OITAVA– FORO ([art. 92, §1º](#))

18.1. Fica eleito o foro da Justiça Federal de Vitória – Seção Judiciária do Espírito Santo para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme [art. 92, §1º, da Lei nº 14.133/21](#).

Vitória, ____ de _____ de 202X.

PRESIDENTE CRCES

CONTRATADA



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 21/08/2025, às 18:03, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0985550** e o código CRC **78D15E0A**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0985550

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

À Pregoeira,

Solicito que sejam adotadas as demais providências necessárias para o regular prosseguimento do processo licitatório.

A CAF, para análise



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 22/08/2025, às 08:44, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0985663** e o código CRC **B1422BEF**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 0985663

PORTARIA SEGEP.PR Nº 83, DE 13 DE ABRIL DE 2023

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 20ª REGIÃO, no uso de suas atribuições legais e regimentais, considerando o contido no PROAD Nº 1895/2023, resolve:

1. Designar o servidor JOSEVAL DE SOUZA LISBOA, Técnico Judiciário - Área Administrativa do Quadro Permanente de Pessoal da Secretaria deste Tribunal, bacharel em Direito, para exercer a Função Comissionada de ASSISTENTE DE DIRETOR DE SECRETARIA (FC-5) da VARA DO TRABALHO DE LAGARTO;
2. Esta Portaria entra em vigor na data de publicação no Diário Oficial da União.

JOSÉ AUGUSTO DO NASCIMENTO

PORTARIA SEGEP.PR Nº 84, DE 13 DE ABRIL DE 2023

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 20ª REGIÃO, no uso de suas atribuições legais e regimentais, considerando o contido no PROAD Nº 1905/2023, resolve:

1. Dispensar a servidora LETÍCIA MARIA BARRETO SAMPAIO, Técnico Judiciário - Área Administrativa do Quadro Permanente de Pessoal da Secretaria deste Tribunal, da função comissionada de ASSISTENTE DE JUIZ (FC-5) da SECRETARIA DA CORREGEDORIA, ficando removida para a 6ª VARA DO TRABALHO DE ARACAJU;
2. Designar o servidor ANDERSON SANTOS DA SILVA, Técnico Judiciário - Área Administrativa do Quadro Permanente de Pessoal da Secretaria deste Tribunal, para exercer a função comissionada de ASSISTENTE DE JUIZ (FC-5) da SECRETARIA DA CORREGEDORIA, passando a ter exercício na referida unidade, ficando dispensado da função comissionada de ASSISTENTE DE DIRETOR DE SECRETARIA (FC-5) da VARA DO TRABALHO DE ITABAIANA;
3. Esta Portaria entra em vigor na data de publicação no Diário Oficial da União.

JOSÉ AUGUSTO DO NASCIMENTO

TRIBUNAL REGIONAL DO TRABALHO DA 21ª REGIÃO

DIRETORIA-GERAL

SECRETARIA ADMINISTRATIVA

ATO Nº 95, DE 12 DE ABRIL DE 2023

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 21ª REGIÃO, no uso de suas atribuições, e de acordo com o constante do PROAD Nº 1032/2023, resolve:

APOSENTAR voluntariamente, com proventos integrais (35/35), o servidor CÂNDIDO OTÁCILIO NOGUEIRA, matrícula nº 308.21.0832, no cargo efetivo da carreira judiciária de Analista Judiciário, Área Administrativa, Sem Especialidade, nível superior, Classe "C", Padrão 13, nº 109, do Quadro Permanente de Pessoal da Secretaria deste Tribunal, de acordo com o art. 3º da Emenda Constitucional nº 47/2005, c/c o art. 3º, § 1º, da Emenda Constitucional nº 103/2019, compostos do vencimento do cargo efetivo, da Gratificação de Atividade Judiciária, de acordo com o art. 13 da Lei nº 11.416/2006, com a redação dada pela Lei nº 13.317/2016, incidente sobre o vencimento básico, mais as seguintes vantagens: 7,5% (sete vírgula cinco por cento) de Adicional de Qualificação, de acordo com o art. 14, § 4º, e art.15, inciso III, da Lei nº 11.416/2006, alterada pela Lei nº 13.317/2016, c/c o anexo I, da Portaria Conjunta nº 1/2007; 17% (dezesete por cento) de Adicional por Tempo de Serviço, conforme art. 67 da Lei nº 8.112/1990; 5/5 (cinco quintos) da Função Comissionada de Responsável pelo Setor de Notificações, Ofícios e Expedições, nível FC 02, incorporados a título de Vantagem Pessoal Nominalmente Identificada, nos termos dos §§ 1º e 2º do art. 15 da Lei nº 9.527/1997, c/c os artigos 2º e 13 da Lei nº 9.624/1998.

ERIDSON JOÃO FERNANDES MEDEIROS

ATO Nº 96, DE 12 DE ABRIL DE 2023

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 21ª REGIÃO, no uso de suas atribuições, e de acordo com o constante do PROAD Nº 1199/2023, e do Acórdão nº 1507/2023, da 1ª Câmara do Tribunal de Contas da União, prolatado no Processo TC nº 004.885/2022-8, resolve:

REVISAR os proventos de NÍSIA AZEVEDO SILVA, servidora aposentada deste Tribunal, no cargo de TÉCNICO JUDICIÁRIO, Área Administrativa, matrícula nº 308.21.0514, reduzindo o percentual de Adicional por Tempo de Serviço, de 07% (sete por cento) para 06% (seis por cento).

ERIDSON JOÃO FERNANDES MEDEIROS

PORTARIA Nº 200, DE 12 DE ABRIL DE 2023

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 21ª REGIÃO, no uso de suas atribuições legais e regimentais, Considerando as disposições contidas no artigo 21, inciso XV, do Regimento Interno;

Considerando os termos do Ofício GDRE n. 003/2023, resolve:

I - Designar os substitutos de SHEILA MARISE DE MEDEIROS FERNANDES, matrícula 308.21.0916, Assessora-Chefe de Gabinete (CJ-03), do Gabinete do Desembargador Ricardo Luís Espíndola Borges, em suas ausências, impedimentos legais e na hipótese de vacância do cargo, na forma abaixo descrita:

1º JOSÉ WALDERY DE SOUZA PARANHOS - 308.21.1008

2º ANA CLÁUDIA MAIA DE MEDEIROS - 308.21.9436

3º DIANA LINHARES TASSINO DE ARAÚJO BARROS - 308.21.9376

II - Esta Portaria entra em vigor na data da sua publicação, revogando-se as disposições em contrário.

ERIDSON JOÃO FERNANDES MEDEIROS

TRIBUNAL REGIONAL DO TRABALHO DA 22ª REGIÃO

PORTARIA GP Nº 268, DE 12 DE ABRIL DE 2023

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 22ª REGIÃO, no uso de suas atribuições legais e regimentais e tendo em vista o Processo Administrativo (PROAD) nº 50/2023, resolve:

Conceder pensão vitalícia a JORGE ANTÔNIO DE CASTRO RISO, na qualidade de cônjuge da servidora JEANE CHAVES RISO, ocupante do cargo Técnico Judiciário, Área Administrativa, Especialidade Cálculo - matrícula 308.22.552 (SGRH - 5457) do quadro de pessoal deste Tribunal Regional do Trabalho da 22ª Região, falecida na atividade, em 31/12/2022, com fundamento nos artigos 217 a 219 da Lei 8.112/90; 23 e 24 da Emenda Constitucional nº 103/2019; artigos 16, inciso I, 74, inciso I, 77, § 2º, incisos II e V, alínea "c", sub-alínea 6 da Lei nº 8.213/1991, com redação integrada pela Portaria ME nº 424, de 30/12/2020 e a recente Portaria SGP/SEDGG/ME nº 4.645, de 24/05/2022, em especial, o contido nos arts. 3º, 6º, 7º, 17 a 20, 24 e 25, 30, 31 e 38, com efeitos a contar de 31/12/2022.

MARCO AURÉLIO LUSTOSA CAMINHA

TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

PORTARIA TRT/GP/DG Nº 234, DE 13 DE ABRIL DE 2023

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições legais e regimentais, resolve:

Nomear a candidata GABRIELA VIEIRA RODRIGUES, aprovada em concurso público homologado por este Tribunal no ano de 2017, em 148º lugar da lista de ampla concorrência, nos termos do art. 9º, inciso I e art. 10, da Lei nº 8.112, de 11 de dezembro de 1990 para exercer, em caráter efetivo, o cargo da carreira judiciária de TÉCNICO JUDICIÁRIO - Área Administrativa, Nível Intermediário, Classe "A", Padrão 1, do quadro permanente de pessoal deste Tribunal, até então ocupado pela servidora ALICE RAQUEL FERREIRA CAVALCANTI GONÇALVES PEREIRA, que, por intermédio da Portaria TRT/GP/DG/229/2023, publicada em 13 de abril de 2023, no DOU nº 71, Seção 2, página 74, tornou-se vago em decorrência de vacância por posse em outro cargo inacumulável, nos termos do artigo 33, inciso VIII da Lei nº 8.112, de 11 de dezembro de 1990, bem como pela desistência expressa da nomeação de Felipe Dias Kohnert Seidler.

JOÃO MARCELO BALSANELLI- Desembargador

PORTARIA TRT/GP/DG Nº 237, DE 13 DE ABRIL DE 2023

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições legais e regimentais, resolve:

Tornar sem efeito a nomeação da candidata LARISSA ALCANTARA FREIRE, para o cargo de TÉCNICO JUDICIÁRIO - Área Administrativa, Nível Intermediário, Classe "A", Padrão 1, ocorrida por intermédio da Portaria TRT/GP/DG 220/2023, publicada no Diário Oficial da União, número 70, seção 2, página 76, de 12/04/2023, em virtude de desistência expressa da posse.

JOÃO MARCELO BALSANELLI- Desembargador

PORTARIA TRT/GP/DG Nº 238, DE 13 DE ABRIL DE 2023

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições legais e regimentais, resolve:

Nomear a candidata VANESSA MASSON VIEIRA, aprovada em concurso público homologado por este Tribunal no ano de 2017, em 149º lugar da lista de ampla concorrência, nos termos do art. 9º, inciso I e art. 10, da Lei nº 8.112, de 11 de dezembro de 1990 para exercer, em caráter efetivo, o cargo da carreira judiciária de TÉCNICO JUDICIÁRIO - Área Administrativa, Nível Intermediário, Classe "A", Padrão 1, do quadro permanente de pessoal deste Tribunal, até então ocupado pela servidora CLAUDIA GISELI VILELA MARQUES, que, por intermédio da Portaria TRT/GP/DG/109/2023, publicada em 1 de março de 2023, no DOU nº 41, Seção 2, página 116, tornou-se vago em decorrência de aposentadoria, nos termos do artigo 33, inciso VII da Lei nº 8.112, de 11 de dezembro de 1990, bem como pela desistência expressa da posse de Larissa Alcântara Freire.

JOÃO MARCELO BALSANELLI- Desembargador

Entidades de Fiscalização
do Exercício das Profissões Liberais

CONSELHO FEDERAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL

PORTARIA Nº 108, DE 13 DE ABRIL DE 2023

O PRESIDENTE DO CONSELHO FEDERAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL, no uso das atribuições que lhe são conferidas pela Lei Federal nº 6.316/1975 e pela Resolução-COFFITO nº 413/2012, resolve:

Art. 1º Exonerar THAISE BRASIL DE MORAES do cargo de Assessora Especial da Presidência do Conselho Federal de Fisioterapia e Terapia Ocupacional, nível I, na data de 13 de abril de 2023.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

ROBERTO MATTAR CEPEDA

CONSELHO FEDERAL DOS TECNICOS INDUSTRIAIS

PORTARIA Nº 59, DE 10 DE ABRIL DE 2023

O PRESIDENTE DO CONSELHO FEDERAL DOS TÉCNICOS INDUSTRIAIS - CFT, no uso das suas atribuições que lhe conferem a Lei 13.693 de 26 de março de 2018, resolve:

Exonerar, a pedido, o Sr. Marcos dos Santos Silva, CPF nº xxx.783.xxx-60 do cargo de Analista de Tecnologia da Informação Júnior do CFT, a partir de 28 de fevereiro de 2023;

Exonerar, a pedido, a Sra. Thais dos Santos Barbosa França, CPF nº xxx.203.xxx-69 do cargo de Técnico Industrial Júnior do CFT, a partir de 29 de março de 2023;

Exonerar, a pedido, o Sr. Victor Francisco Braga Tavares, CPF nº xxx.192.xxx-21 do cargo de Assistente Administrativo I do CFT, a partir de 31 de março de 2023;

Exonerar, a pedido, o Sr. Gilberto Pereira da Rocha, CPF nº xxx.727.xxx-91 do cargo de Analista Técnico Júnior do CFT, a partir de 10 de abril de 2023.

SOLOMAR PEREIRA ROCKEMBACH

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

PORTARIA DO CRCES Nº 27, DE 13 DE ABRIL DE 2023

A PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO, no uso de suas atribuições legais e regimentais; CONSIDERANDO o disposto no art. 8º da Lei nº 14.133, de 1º de abril de 2021, resolve:

Art. 1º. Designar para desempenho das funções de Agente de Contratação e Pregoeiro, aptos a tomarem decisões, acompanharem o trâmite das licitações, darem impulso aos procedimentos licitatórios e executarem quaisquer outras atividades necessárias ao bom andamento dos certames até a homologação os seguintes empregados: a) Agente de Contratação Titular: Amylene Shneider Gonçalves Delunardo; b) Agente de Contratação Suplente: Grazielly Inácio Tartaglia. Art. 2º. Designar como integrantes da Equipe de Apoio os seguintes empregados: a) Douglas Ferrari Junior; b) Erika de Oliveira Correa; e c) Roberto Luciano Soares Gomes. Parágrafo único. Os empregados mencionados no caput deste artigo auxiliarão o Agente de Contratação no desempenho de suas atribuições, em conjunto ou isoladamente. Art. 3º. A Presidência da Comissão de Contratação incumbirá à Amylene Shneider Gonçalves Delunardo, que, em suas ausências e/ou impedimentos, será substituída pela empregada Grazielly Inácio Tartaglia. Art. 4º. Em licitação que envolva bens ou serviços especiais, desde que observados os requisitos estabelecidos na Lei nº 14.133/2021, o Agente de Contratação poderá ser substituído por Comissão de Contratação formada por no mínimo 3 (três) membros, especialmente designados, que responderão, solidariamente, por todos os atos praticados pela comissão, ressalvado o membro que expressar posição individual

divergente fundamentada e registrada em ata lavrada em reunião que houver sido tomada a decisão. Art. 5º. O Agente de Contratação, equipe de apoio ou a Comissão de Contratação possuem a prerrogativa de solicitar Assessoramento Jurídico e de Controle Interno para o desempenho das funções essenciais à execução do disposto na Lei nº 14.133/2021 e suas alterações. Art. 6º. O Agente de Contratação e/ou Comissão de Contratação poderá convocar empregados que possuam conhecimento técnico acerca do objeto da licitação ou contratação direta, para auxiliarem quanto às especificidades de propostas e documentos de habilitação. Parágrafo único. Nas contratações que envolvam



bens ou serviços especiais cujo objeto não seja rotineiramente contratado pela administração, poderá ser contratado, por prazo determinado, serviço de empresa ou de profissional especializado para assessorar os agentes públicos responsáveis pela condução da licitação. Art. 7º. Os Agentes de Contratação e a Equipe de Apoio deverão adotar o Decreto nº 11.246, de 27 de outubro de 2022, o qual regulamenta o disposto no § 3º do art. 8º da Lei nº 14.133, de 1º de abril de 2021, que dispõe sobre as regras para a atuação do Agente de Contratação e da Equipe de Apoio, o funcionamento da Comissão de Contratação e a atuação dos Gestores e Fiscais de Contratos, no âmbito da Administração Pública Federal direta, autárquica e fundacional. Art. 8º. Esta Portaria entra em vigor na data de sua publicação.

CARLA CRISTINA TASSO

CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO

PORTARIA COREN-RJ N.º 755, DE 3 DE ABRIL DE 2023

A Presidente do Conselho Regional de Enfermagem do Rio de Janeiro, juntamente com a Primeira Secretária da Autarquia, no uso de suas atribuições legais e regimentais conferidas na Resolução Cofen nº 421/2012, que aprova o Regimento Interno da Autarquia;

CONSIDERANDO: 1. Os termos do artigo 37, II da Constituição Federal que prevê a livre nomeação e exoneração de servidores para cargos em comissão no âmbito da Administração Pública, resolve:

Art.1º. Exonerar RODRIGO GUANABARA MOREIRA do cargo em comissão de ASSESSOR TÉCNICO NÍVEL IV, a partir de 03/04/2023.

Art.2º. Esta portaria entrará em vigor na data de sua assinatura, produzindo efeitos administrativos e financeiros a partir desta data, revogando as disposições em contrário.

LILIAN PRATES BELEM BEHRING
Presidente do COREN

GLACY KELLY GOMES DA CUNHA BISAGGIO
Primeira Secretária COREN

PORTARIA COREN-RJ Nº 760, DE 3 DE ABRIL DE 2023

A Presidente do Conselho Regional de Enfermagem do Rio de Janeiro, juntamente com a Primeira Secretária da Autarquia, no uso de suas atribuições legais e regimentais conferidas na Resolução Cofen nº 421/2012, que aprova o Regimento Interno da Autarquia;

CONSIDERANDO: 1. Os termos do artigo 37, II da Constituição Federal que prevê a livre nomeação e exoneração de servidores para cargos em comissão no âmbito da Administração Pública; resolve:

Art.1º. Exonerar ANDRESSA SANTOS DE OLIVEIRA do cargo em comissão de ASSESSOR TÉCNICO NÍVEL VI, a partir de 03/04/2023.

Art.2º. Esta portaria entrará em vigor na data de sua assinatura, produzindo efeitos administrativos e financeiros a partir desta data, revogando as disposições em contrário.

LILIAN PRATES BELEM BEHRING
Presidente do COREN

GLACY KELLY GOMES DA CUNHA BISAGGIO
Primeira Secretária COREN

PORTARIA COREN-RJ Nº 773, DE 4 DE ABRIL DE 2023

A Presidente do Conselho Regional de Enfermagem do Rio de Janeiro, juntamente com a Primeira Secretária da Autarquia, no uso de suas atribuições legais e regimentais conferidas na Resolução Cofen nº 421/2012, que aprova o Regimento Interno da Autarquia;

CONSIDERANDO: 1.Os termos do artigo 37, II da Constituição Federal que prevê a livre nomeação e exoneração de servidores para cargos em comissão no âmbito da Administração Pública; 2.O deliberado pela Presidência no Memorando nº 205/2023 - Presidência, resolve:

Art.1º. Nomear JULIANA GONÇALVES MONTEIRO para cargo em comissão de ASSESSOR TÉCNICO NÍVEL VI, a partir de 04/04/2023.

Art.2º. Esta portaria entrará em vigor na data de sua assinatura, produzindo efeitos administrativos e financeiros a partir da data supracitada.

LILIAN PRATES BELEM BEHRING
Presidente do COREN

GLACY KELLY GOMES DA CUNHA BISAGGIO
Primeira Secretária COREN

CONSELHO REGIONAL DE ENFERMAGEM DE RORAIMA

PORTARIA Nº 32, DE 15 DE FEVEREIRO DE 2023

A Presidente juntamente com a secretária do Conselho Regional de enfermagem de Roraima, no uso de suas atribuições que lhe são conferidas pela lei nº 5.905/73 e pelo Regimento Interno desta Autarquia.

Considerando a necessidade de contratação de pessoal para preencherem os cargos vagos de e os que vierem a ser criados de provimento efetivo;

Considerando a deliberação do Plenário na 87ª ROP (Reunião Ordinária de Plenário) em 18 de janeiro de 2023, resolvem:

Art. 1º - INSTITUIR a comissão do concurso público do COREN-RR, destinado à seleção de candidatos para provimento dos cargos públicos do quadro efetivo para provimento dos cargos públicos efetivos.

Art.2º - A comissão fica encarregada de fazer o estudo técnico, com apresentação dos cargos, as atribuições de cada cargo, os vencimentos básicos, os benefícios e o impacto financeiro.

Art. 3º - Ficam DESIGNADOS para a composição da comissão a conselheira e os empregados públicos relacionados abaixo:

- I - Erika Madelaine Souza do Nascimento Carvalho;
- II - Donária Santana da Cruz Neta;
- II - Carlete Alves Abreu, e;
- IV - Frederico Junior Pereira Evangelista.

Parágrafo Único - A comissão irá reunir-se 01 (uma) vez por semana, nas quintas-feiras, com o prazo de 90 (noventa) dias para a conclusão dos trabalhos e apresentação do estudo técnico do caput deste artigo.

Art. 4º - Esta portaria entra em vigor na data da sua publicação.

TARCIA MILLENE DE A. COSTA BARRETO
Presidente

GABRIELLE DE ALMEIDA RODRIGUES
Secretária

CONSELHO REGIONAL DE MEDICINA VETERINÁRIA DO ESTADO DE MINAS GERAIS

PORTARIA Nº 8 DE 1º DE MARÇO DE 2023

O Presidente do Conselho Regional de Medicina Veterinária do Estado de Minas Gerais (CRMV-MG) no uso da atribuição que lhe confere a letra "j" do artigo 17 do seu Regimento Interno, baixado pela Resolução CRMV-MG nº 342, de 1º de fevereiro de 2011, aprovada pela Decisão do egrégio Conselho Federal de Medicina (CFMV), publicada no Diário Oficial da União, Seção I, de 11 de agosto de 2011, à página 112, resolve:

Art. 1º - Fica constituída a Comissão de Contratação composta pelos Agentes de Contratação e pela Equipe de Apoio para a realização de Licitações nas suas diversas modalidades para o Conselho Regional de Medicina Veterinária do Estado de Minas Gerais (CRMV-MG).

Art. 2º - A Comissão será constituída por 6 (seis) servidores do Quadro de Pessoal Permanente do CRMV-MG, sendo que 3 (três) deles atuarão em caráter efetivo e os outros 3 (três) como suplentes, a seguir designados:

Nome	Designação
Joaquim Paranhos Amancio	Agente de Contratação
Eron Januário da Silva	Agente de Contratação
Equipe de Apoio	
Luana Grasielle Martins Ribeiro Sousa	Membro Efetivo
Tânia dos Santos Teixeira Lima	Membro Efetivo
Ana Maurina Carvalho	Membro Suplente
Miriam Imaculada Lopes Fernandes	Membro Suplente

§ 1º - O mandato dos membros da Comissão é de 2 (dois) anos, devendo os servidores designados exercer estas atividades sem prejuízo das funções de seus respectivos cargos.

§ 2º - O Agente de Contratação, conforme a modalidade de licitação a se realizar, será substituído, em sua ausência ou impedimento, pelo respectivo Suplente.

§ 3º - As ausências, os impedimentos e as substituições serão sempre objeto de registro nas Atas da Comissão Permanente de Licitação e da Equipe de Apoio de Pregão.

§ 4º - O membro suplente será convocado pelo Presidente ou Pregoeiro para substituir membro efetivo ausente ou para compor Equipe, de acordo com a complexidade da Contratação.

Art. 3º - Compete à Comissão de Contratação praticar todos os atos necessários à expedição dos Editais, organização, recebimento, exame e julgamento dos documentos e procedimentos relativos às licitações, em qualquer de suas modalidades, mediante a classificação das propostas, submetendo-as para homologação, revogação ou anulação do Presidente desta Autarquia, de acordo com o disposto na Lei nº. 14.133, de 1º de abril de 2021, e na legislação complementar.

Parágrafo único. A Comissão de Contratação reunir-se-á em local, dia e hora que o Agente de Contratação designar, sendo necessário o "quorum" mínimo de 3 (três) membros para processar e julgar as propostas.

Art. 4º - À Comissão de Contratação é assegurada competência para convocar profissional com conhecimento técnico, visando o necessário assessoramento e emissão de Parecer especializado, referente ao objeto da licitação.

Art. 5º - Esta Portaria entra em vigor na data de sua publicação.

BRUNO DIVINO ROCHA

PORTARIA Nº 37, DE 12 DEZEMBRO DE 2022

O CONSELHO REGIONAL DE MEDICINA VETERINÁRIA DO ESTADO DE MINAS GERAIS (CRMV-MG), no uso da atribuição que lhe confere as letras "g", "i", "k" e "l" do artigo 17 do seu Regimento Interno, baixado pela Resolução nº 342, de 1º de fevereiro de 2011, aprovado pela Decisão do egrégio Conselho Federal de Medicina Veterinária (CFMV), publicada no Diário Oficial da União - Seção 1, na página 112, do dia 11 de agosto de 2011,

considerando a criação do Cargo em Comissão de Analista de Mídias Sociais, ocorrido na 522ª Reunião Plenária deste CRMV-MG, realizada em 20 de dezembro de 2019, resolve:

Art. 1º - Nomear Daniela Ferreira Campos para ocupar o Cargo em Comissão de Analista de Mídias Sociais, de recrutamento amplo e de livre nomeação e exoneração do Presidente do Conselho Regional de Medicina Veterinária do Estado de Minas Gerais (CRMV-MG).

Art. 2º - O salário para o Cargo em Comissão de Analista de Mídias Sociais é de R\$3.264,63 (três mil duzentos e sessenta e quatro reais e sessenta e três centavos), com reajuste anual na data base dos empregados do CRMV-MG.

Art. 3º - Esta Portaria entra em vigor a partir de 12 de dezembro de 2022.

BRUNO DIVINO ROCHA
Presidente do Conselho

CONSELHO REGIONAL DE NUTRICIONISTAS DA 9ª REGIÃO

ATO Nº 20, DE 13 DE ABRIL DE 2023

A Presidenta do Conselho Regional de Nutricionistas da 9ª Região, no uso de suas atribuições legais, resolve:

Nomear, em caráter efetivo, em virtude de sua aprovação no concurso público, de que trata o edital CRN9 01/2019, cujo resultado final foi homologado e publicado no DOU em 20/02/2020, o seguinte candidato para o cargo do CRN9 abaixo relacionado.

NUTRICIONISTA FISCAL –BARBACENA
CPF: 118.479.856-70 - ANDRESA CAROLINA DA SILVA COSTA
NUTRICIONISTA FISCAL –BELO HORIZONTE
CPF: 062.899.076-62 - DAYANA CRISTINA BRITO

ERIKA SIMONE COELHO CARVALHO

CONSELHO REGIONAL DOS TÉCNICOS INDUSTRIAIS DO ESTADO DA BAHIA

PORTARIA Nº 4, DE 24 DE JANEIRO DE 2023

O CONSELHO REGIONAL DOS TÉCNICOS INDUSTRIAIS DO ESTADO DA BAHIA, no uso das competências que lhe confere a Lei nº 13.639 de 2018 e o Regimento Interno.

CONSIDERANDO que os Conselhos de Técnicos Industriais são entidades criadas por lei, com atribuições de fiscalizar e normatizar o exercício profissional do técnico industrial, mantidas com recursos próprios e não receptoras de subvenções ou transferências advindas do Orçamento da União, resolve:

Art. 1º. Alterar cargos de livre provimento e demissão, a partir do dia 02 de janeiro de 2023:

I. Sr.(a) FRANCISCO DE ASSIS SANTANA LEITE (CPF: XXX.965.XXX-72), sob a MATRÍCULA n. 0046, terá seu cargo alterado para ASSESSOR II.

Art. 2º. Esta Portaria entrará em vigor a partir da data de sua assinatura.

SANDRO AUGUSTO VIEIRA DA SILVA
Presidente do CRT-BA





CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

PROCESSO Nº 9079618110000798.000048/2025-57

CHECKLIST DO PROCESSO LICITATÓRIO.

(X) Documento de Formalização de Demanda – DFD;

(X) Portaria nomeação de Equipe de planejamento;

(X) Estudo Preliminar;

(X) Mapa de Riscos;

(X) Termo de Referência;

(X) Cotação de preços / Mapa de estimativa;

() Reserva / Dotação orçamentária - consta apenas justificativa da impossibilidade, neste período desse exercício, da emissão da reserva orçamentária ou apresentação do plano orçamentário aprovado pelo Conselho Federal de Contabilidade e da justificativa da necessidade do prosseguimento do processo por tratar-se de serviço contínuo;

(X) Autorização da Autoridade Competente.



Documento assinado eletronicamente por **Amylene Shneider Gonçalves Delunardo, Assistente**, em 09/09/2025, às 15:36, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1012405** e o código CRC **042839EA**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

À Assessoria Jurídica do CRCES

Em cumprimento ao art. 53 da Lei nº 14.133/2021 - NLLC, encaminho os autos para análise jurídica e emissão de parecer:

Art. 53. Ao final da fase preparatória, o processo licitatório seguirá para o órgão de assessoramento jurídico da Administração, que realizará controle prévio de legalidade mediante análise jurídica da contratação."

Ratifico que os requisitos estabelecidos no inciso IX do art. 18 da NLLC foram estabelecidos pelo Setor Requisitante, conforme consta no Termo de Referência e que não consta a reserva orçamentária nos autos, tendo o área requisitante apresentado justificativa conforme documento SEI nº 985529.

Identifiquei que faltam assinaturas no ETP e mapa de riscos, além do ETP ter descrita a composição diferente do DFD; e a necessidade de ajuste no item referente a qualificação técnica que está sendo exigida, agrupando exigências pontuais de apresentação de documentos (atestados) e correção da numeração dos itens.



Documento assinado eletronicamente por **Amylene Shneider Gonçalves Delunardo, Assistente**, em 09/09/2025, às 16:13, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1012518** e o código CRC **730B1CE3**.

PARECER JURÍDICO n.º 94/2025.

Processo: 90796181100000798.000048/2025-57

Interessado: Setor Administrativo e Departamento de Tecnologia da Informação do CRCES.

Assunto: Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

PREGÃO ELETRÔNICO. LEI Nº 14.133/2021. SERVIÇOS GERENCIADOS EM TECNOLOGIA DA INFORMAÇÃO, INSTALAÇÃO E GESTÃO DE REDE WI-FI, FIREWALL DE PRÓXIMA GERAÇÃO, BACKUP LOCAL E EM NUVEM E SUPORTE TÉCNICO. ANÁLISE JURÍDICA DO PROCEDIMENTO E DE MINUTAS. Possibilidade jurídica do uso de pregão quando o objeto possuir padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital. Recomendações.

I. RELATÓRIO:



Os autos foram encaminhados pela Agente de Contratação do CRCES, denominada Pregoeira, para "análise jurídica e emissão de parecer", em cumprimento ao artigo 53 da Lei nº 14.133/2021 (**ID 1012518**).

O Documento de Formalização de Demanda - DFD (**ID 0929590**) indica como objeto a "*Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.*"

O Estudo Técnico Preliminar (ETP) realizado (**ID 0930157**) **DECLARA:** "*Com base nas informações estabelecidas neste documento, nas justificativas apresentadas no Documento de Formalização da Demanda – DFD, a Equipe de Planejamento **DECLARA a viabilidade da contratação de empresa especializada**, Serviços de TI inclui a gestão de redes, ativos de rede, servidores, estações de trabalho, nobreaks e monitores. A empresa será responsável por suporte técnico remoto e presencial, manutenção preventiva e corretiva, e monitoramento de links de internet e infraestrutura hiperconvergente.*"

Foi realizada Análise de Riscos da fase de planejamento da contratação (**ID 0952056**).

Juntou-se o "Termo de Referência de TIC" (**ID 0962132**), do qual se extrai que o objeto do certame é a "Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. (...)." (**Item 1.1**).

A pesquisa de preço de mercado (**ID 0974302**) é obtida por orçamento fornecido por 03 (três) potenciais fornecedores. O Mapa Comparativo de



Preços é apresentado em **ID 0974303**, acompanhado de Despacho de Conclusão de Pesquisa de Preços em **ID 0974305**.

Observa-se, ainda, Autorização e Justificativa da Presidência do CRCES (**ID 0985548**), Despacho de pedido de reserva (**ID 0985529**), Nota de designação de Agente de Contratação e Pregoeiro pela edição da Portaria CRCES nº 27, de 13 de abril de 2023 (**ID 1012399**), Checklist do Processo Licitatório (**ID 1012405**), Minuta de Contrato (**ID 0985550**) e Minuta de Edital (**ID 1012514**).

Por fim, há nos autos o Despacho de encaminhamento do processo para análise jurídica (**ID 1012518**).

É o relatório, no essencial, passo a opinar.

II. FUNDAMENTAÇÃO:

II.A – NOTAS INTRODUTÓRIAS SOBRE LIMITES DA ATUAÇÃO NO PARECER JURÍDICO.

Cabe enfatizar, inicialmente, que a vertente análise toma por base, exclusivamente, os elementos constantes dos autos e da consulta formulada, limitando-se aos aspectos jurídico-formais e desconsiderados a conveniência e oportunidade do ato, que estão reservados à esfera discricionária do administrador público, ou aspectos técnicos, econômico-financeiros e administrativos pertinentes à mesma, uma vez que fogem ao exame jurídico próprio dos órgãos de consultoria administrativa.

Saliento, ademais, que **este parecer será fundamentado exclusivamente nas disposições da Lei 14.133/2021**, pois esse foi o diploma regente do procedimento licitatório inicial, de modo que, eventualmente, em havendo citação à lei anterior (Lei n.º 8.666/1993) para fins de comparativo, o presente opinativo fará referência expressa.



Dessa forma, para evitar a reprodução excessiva do número da revogada Lei de Licitações, antecipo que quando este opinativo fizer referência apenas ao “número de artigo entre parênteses”, referir-se-á a dispositivo da Lei n. 14.133/2021.

Alertamos, por fim, que **a verificação de erros materiais, como a remissão a itens equivocados ou de grafia, é atividade que extrapola a análise jurídica**, objeto do presente parecer. Se eventuais observações forem tecidas, serão apenas aquelas que se evidenciarem no curso da leitura, não tendo, pois, qualquer caráter exaustivo.

II.B – MODALIDADE DE LICITAÇÃO ESCOLHIDA.

O art. 6º, XLI da Lei 14.133/21 estabelece que o pregão será a ***“modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto”***. Assim dispõe o art. 29 do mesmo diploma:

Art. 29. A concorrência e o pregão seguem o rito procedimental comum a que se refere o art. 17 desta Lei, adotando-se o **pregão** sempre que o objeto possuir **padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital**, por meio de especificações usuais de mercado.

Saliente-se que, de acordo com a **Orientação Normativa nº 54**, de 2014, da Advocacia-Geral da União, incumbe ao agente ou ao setor técnico da administração o encargo de declarar que o objeto licitatório é de natureza comum capaz de ser licitado por pregão:

Compete ao **agente ou setor técnico da administração declarar que o objeto licitatório é de natureza comum** para efeito de utilização da modalidade pregão e definir se o objeto corresponde a obra ou serviço de engenharia, sendo atribuição do órgão jurídico analisar o devido enquadramento da modalidade licitatória aplicável.

No caso em apreço, o objeto licitado é a contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação, conforme descrito no DFD e no TR **(ID 0962132)**.



Nesse sentido, verifica-se que há indicação de que o objeto é de **natureza comum** apenas no Documento de Formalização da Demanda e no Estudo Técnico Preliminar, razão pela qual recomendo a inserção desta indicação no **TR (ID 0962132)**, bem como na **minuta do Edital de Id. 1012514. [RECOMENDAÇÃO 01]**.

Ressaltamos, ainda, que fora editada a **Instrução Normativa SEGES/ME nº 73**, de 30 de setembro de 2022, que *"dispõe sobre a licitação pelo critério de julgamento por menor preço ou maior desconto, na forma eletrônica, para a contratação de bens, serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional"*. Essa normativa deve ser observada pelo Agente de Contratação do CRCES na condução do procedimento licitatório em foco.

III. INSTRUÇÃO PROCESSUAL:

III.A – DAS FORMALIDADES GERAIS

O Pregão Eletrônico é modalidade de licitação a ser processada pelo rito procedimental comum (art. 17) e sua **fase preparatória está disciplinada no Título II, Capítulo II**, entre os artigos 18 a 52.

O art. 18, abaixo transcrito com grifos nossos, estabelece os elementos compreendidos na fase preparatória da licitação:

Art. 18. *A fase preparatória do processo licitatório é caracterizada pelo planejamento e deve **compatibilizar-se** com o plano de contratações anual de que trata o inciso VII do caput do art. 12 desta Lei, sempre que elaborado, e com as leis orçamentárias, bem como **abordar** todas as considerações técnicas, mercadológicas e de gestão que podem interferir na contratação, **compreendidos:***

- I - a descrição da necessidade da contratação fundamentada em **estudo técnico preliminar** que caracterize o interesse público envolvido;*
- II - a definição do objeto para o atendimento da necessidade, por meio de **termo de referência**, anteprojeto, projeto básico ou projeto executivo, conforme o caso;*



III - a definição das condições de execução e pagamento, das garantias exigidas e ofertadas e das condições de recebimento;

IV - o orçamento estimado, com as composições dos preços utilizados para sua formação;

*V - a elaboração do **edital de licitação**;*

*VI - a elaboração de **minuta de contrato**, quando necessária, que constará obrigatoriamente como anexo do edital de licitação;*

VII - o regime de fornecimento de bens, de prestação de serviços ou de execução de obras e serviços de engenharia, observados os potenciais de economia de escala;

VIII - a modalidade de licitação, o critério de julgamento, o modo de disputa e a adequação e eficiência da forma de combinação desses parâmetros, para os fins de seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, considerado todo o ciclo de vida do objeto;

IX - a motivação circunstanciada das condições do edital, tais como justificativa de exigências de qualificação técnica, mediante indicação das parcelas de maior relevância técnica ou valor significativo do objeto, e de qualificação econômico-financeira, justificativa dos critérios de pontuação e julgamento das propostas técnicas, nas licitações com julgamento por melhor técnica ou técnica e preço, e justificativa das regras pertinentes à participação de empresas em consórcio;

*X - a **análise dos riscos** que possam comprometer o sucesso da licitação e a boa execução contratual;*

XI - a motivação sobre o momento da divulgação do orçamento da licitação, observado o art. 24 desta Lei.

Extraem-se do dispositivo legal os atos formais elementares da fase interna da contratação pública, quais sejam, o **estudo técnico preliminar - ETP**, a **análise de riscos** e o **termo de referência - TR** (anteprojeto, projeto básico ou projeto executivo, caso obra ou serviço de engenharia), e necessidade de elaboração de **edital de licitação** e, quando for o caso, a **minuta de contrato**.

A presença e a confecção regular dos atos formais indicados no parágrafo anterior [**ETP, Análise de Riscos, TR, edital e a minuta de contrato**] resultam na constatação de que houve o cumprimento integral do planejamento previsto no artigo 18 da NLL.

A verificação da presença de todos os atos formais da fase de planejamento está verificada nos autos, conforme se consta do preenchimento do



checklist de **ID 1012405**. Independentemente da análise empreendida, cabe ao Agente Público responsável pela contratação verificar se todos os documentos acima estão presentes nos autos.

Em capítulos que se seguem abaixo proceder-se-á a análise da regular confecção desses atos e da inserção de seu conteúdo obrigatório para confirmação do preenchimento dos requisitos do artigo 18 da Lei 14.133/2021 e da regularidade da instrução processual da fase preparatória.

Entretanto, antes disso, apresentamos breves comentários sobre a presença de atos obrigatórios que não estão indicados no multicitado artigo 18.

Primeiramente, registro a presença de **Autorização Superior de Abertura da Licitação** por meio do Despacho de **ID 0985548**, assim como a designação da Comissão de Planejamento e de Agente de Contratação e Pregoeiro, consoante Portaria CRCES N° 042, de 20 de outubro de 2023 (**ID 0929613**) e cópia da publicação no DOU da Portaria CRCES nº 27, de 24 de maio de 2024 (**ID 1012399**).

A existência de disponibilidade orçamentária com a respectiva indicação da classificação funcional programática e da categoria econômica da despesa é uma imposição legal. Nesse particular, lembramos que deverá ser observado o disposto no art. 60 da Lei 4.320/64¹.

O Termo de Referência reza, em seu item 10.2.:

10.2 A contratação será atendida pela seguinte dotação:
6.3.1.3.02.01.05 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

Há nos autos a manifestação do setor competente para o procedimento de emissão da Reserva Orçamentária, conforme indica o Despacho de Pedido de Reserva de **Id. 0985529**, que observa a necessidade de se emitir a nota de empenho no ano de 2026, quando o contrato em vigência se encerra: A

¹ Art. 60. É vedada a realização de despesa sem prévio empenho.



ausência de reserva orçamentária prévia se justifica pelos seguintes fundamentos: **Vigência contratual atual assegurada:** a infraestrutura tecnológica crítica para as operações do CRCES permanece operante, garantindo a continuidade dos serviços até 31 de janeiro de 2026; **Execução condicionada ao novo exercício:** a nova contratação será executada a partir de fevereiro de 2026, vinculando-se integralmente ao orçamento do exercício seguinte; **Planejamento em andamento:** a despesa já está considerada no planejamento orçamentário institucional em elaboração, cujo Plano de Trabalho será consolidado até setembro de 2025, conforme cronograma oficial; **Previsão de empenho futuro:** os valores referentes à contratação serão regularmente empenhados dentro do orçamento de 2026, em observância aos princípios da responsabilidade fiscal. Cabe destacar que a postergação da fase interna do procedimento licitatório até a aprovação do orçamento de 2026 comprometeria o cronograma necessário para a conclusão regular do certame, trazendo risco de descontinuidade na prestação dos serviços de TI essenciais. Tal cenário impactaria diretamente o funcionamento do CRCES, prejudicando a execução das atividades administrativas e técnicas e comprometendo a continuidade das operações da instituição.

Assim, a continuidade do processo licitatório até as fases de julgamento, homologação e assinatura do contrato revela-se juridicamente adequada, inexistindo impedimento legal para tanto, desde que a execução financeira seja realizada somente após o início da vigência do novo ajuste e observados os limites estabelecidos na Lei Orçamentária Anual de 2026.

Ressalte-se, ainda, que embora a tramitação das fases licitatórias seja juridicamente possível, a formalização do contrato deve estar condicionada à existência de dotação orçamentária suficiente e regular, já consignada na Lei Orçamentária Anual de 2026. Dessa forma, afasta-se qualquer interpretação de que a assinatura contratual poderia ocorrer sem a devida cobertura orçamentária, preservando-se a observância ao princípio da legalidade.

Feitas essas considerações, passamos à análise do atendimento do conteúdo imposto em lei para o Estudo Técnico Preliminar, o Termo de Referência, a Minuta de Edital e a Minuta de Contrato.

III.B – DO ESTUDO TÉCNICO PRELIMINAR



O Estudo Técnico Preliminar – ETP é o “Documento constitutivo da primeira etapa do planejamento de uma contratação que caracteriza o interesse público envolvido e a sua melhor solução e dá base ao anteprojeto, ao termo de referência ou ao projeto básico a serem elaborados caso se conclua pela viabilidade da contratação” (**art. 6º, XX, NLL**).

O Estudo Técnico Preliminar está regulamentado, em nível legal, pelo **artigo 18, §1º da Lei 14.133/2021**. Eis o seu conteúdo elementar:

Art. 18 [...]

§ 1º O estudo técnico preliminar a que se refere o inciso I do caput deste artigo deverá evidenciar o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação, e conterá os seguintes elementos:

I - descrição da **necessidade da contratação**, considerado o problema a ser resolvido sob a perspectiva do interesse público;

II - demonstração da **previsão da contratação no plano de contratações anual**, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração;

III - **requisitos da contratação**;

IV - **estimativas das quantidades** para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala;

V - **levantamento de mercado**, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar;

VI - **estimativa do valor da contratação**, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação;

VII - **descrição da solução como um todo**, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso;

VIII - justificativas para o **parcelamento ou não** da contratação;

IX - demonstrativo dos **resultados pretendidos** em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;

X - providências a serem adotadas pela Administração **previamente à celebração do contrato**, inclusive quanto à capacitação de servidores ou de empregados para fiscalização e gestão contratual;



XI - contratações correlatas e/ou interdependentes;

XII - descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável;

XIII - posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina.

Esses dispositivos foram regulamentados pela **INSTRUÇÃO NORMATIVA SEGES/ME Nº 58**, de 8 de agosto de 2022, que dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital.

Quanto ao conteúdo, a referida IN dispõe que o ETP deve atender aos seguintes requisitos:

Art. 9º Com base no Plano de Contratações Anual, deverão ser registrados no Sistema ETP Digital os seguintes elementos:

I - descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público;

II - descrição dos requisitos da contratação necessários e suficientes à escolha da solução, prevendo critérios e práticas de sustentabilidade, observadas as leis ou regulamentações específicas, bem como padrões mínimos de qualidade e desempenho;

III - levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar, podendo, entre outras opções:

a) ser consideradas contratações similares feitas por outros órgãos e entidades públicas, bem como por organizações privadas, no contexto nacional ou internacional, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da Administração;

b) ser realizada audiência e/ou consulta pública, preferencialmente na forma eletrônica, para coleta de contribuições;

c) em caso de possibilidade de compra, locação de bens ou do acesso a bens, ser avaliados os custos e os benefícios de cada opção para escolha da alternativa mais vantajosa, prospectando-se arranjos inovadores em sede de economia circular; e

d) ser consideradas outras opções logísticas menos onerosas à Administração, tais como chamamentos públicos de doação e permutas.



- IV** - descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso;
- V** - estimativa das quantidades a serem contratadas, acompanhada das memórias de cálculo e dos documentos que lhe dão suporte, considerando a interdependência com outras contratações, de modo a possibilitar economia de escala;
- VI** - estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação;
- VII** - justificativas para o parcelamento ou não da solução;
- VIII** - contratações correlatas e/ou interdependentes;
- IX** - demonstrativo da previsão da contratação no Plano de Contratações Anual, de modo a indicar o seu alinhamento com o instrumentos de planejamento do órgão ou entidade;
- X** - demonstrativo dos resultados pretendidos, em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;
- XI** - providências a serem adotadas pela Administração previamente à celebração do contrato, tais como adaptações no ambiente do órgão ou da entidade, necessidade de obtenção de licenças, outorgas ou autorizações, capacitação de servidores ou de empregados para fiscalização e gestão contratual;
- XII** - descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável; e
- XIII** - posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina.
- § 1º O ETP deverá conter ao menos **os elementos previstos nos incisos I, V, VI, VII e XIII** do caput deste artigo e, **quando não contemplar os demais elementos, apresentar as devidas justificativas.**
- § 2º Caso, após o levantamento do mercado de que trata o inciso III, a quantidade de fornecedores for considerada restrita, deve-se verificar se os requisitos que limitam a participação são realmente indispensáveis, flexibilizando-os sempre que possível.
- § 3º Em todos os casos, o estudo técnico preliminar deve privilegiar a consecução dos objetivos de uma contratação, nos termos no art. 11 da Lei nº 14.133, de 2021, em detrimento de modelagem de contratação centrada em exigências meramente formais.

O ETP colacionado aos autos (**ID 0930157**) atende aos requisitos dos incisos do artigo 18 da Lei nº 14.133/2021 e dos incisos do art. 9º da IN SEGES/ME N° 58, havendo que se atentar apenas à ressalva a seguir.



O ETP descreveu adequadamente, dentre outros elementos, a necessidade de contratação **(item 2.1)**; o levantamento de mercado e a justificativa da escolha do tipo de solução a contratar **(item 2.5)**; a descrição da solução como um todo **(item 2.7)**; justificativas para o não parcelamento do contrato **(item 2.8)**; demonstrativo dos resultados pretendidos, em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis **(item 2.9)**; desnecessidade de providências a serem adotadas pela administração previamente à celebração do contrato **(item 2.10)**; e o posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina, entendendo pela viabilidade da contratação proposta **(item 2.13)**.

A respeito da estimativa do valor da contratação, exigida no inciso VI do dispositivo legal referenciado acima, observa-se que o **item 2.6** do ETP estimou o valor anual de **R\$ 480.000,00 (quatrocentos e oitenta mil reais)**, em razão dos orçamentos obtidos e compilados em Documento de Pesquisa de Preços de **ID 0974302**. Verifica-se, no entanto, que no **item 2.5** do ETP, em que pese haver menção ao valor estipulado para a contratação no item 2.6, alguns de seus subitens estão sem preenchimento, ou com valores genéricos "xxx". Recomenda-se, portanto, sua retificação pelo setor competente **[RECOMENDAÇÃO 02]**

Sabe-se que, em regra, a pesquisa de preços deve ser a mais ampla possível, priorizando: **(i)** preços obtidos em contratações públicas recentes; **(ii)** praticados em outros contratos da Administração Pública, desde que em condições semelhantes; **(iii)** fixados por órgão oficial competente ou constantes do sistema de registro de preços; **(iv)** constantes de publicações e sites especializados, se for o caso; **(v)** outras que julgar pertinente; pois essa tem sido a remansosa orientação do TCU ao longo dos anos, conforme se pode notar do **Acórdão nº 3224/2020-Plenário**.

Lembramos que compete ao setor técnico zelar pela adequação da pesquisa de preços², e que a aquisição por montante incompatível

² "Não constitui incumbência obrigatória da CPL, do pregoeiro ou da autoridade superior realizar pesquisas de preços no mercado e em outros entes públicos, sendo essa atribuição, tendo em vista a complexidade dos diversos objetos licitados, dos setores ou pessoas competentes envolvidos na aquisição do objeto." (**Acórdão nº 3516/2007, Primeira Câmara, Relator Min. Aroldo Cedraz, Processo nº 005.991/2000-7**)



com o mercado pode gerar a responsabilização da unidade técnica especializada³ e da autoridade que homologa o certame⁴.

Insta destacar que a aferição da compatibilidade do preço contratado foge à competência da assessoria jurídica, por se tratar de aspecto econômico-financeiro, recaiando a responsabilidade na indicação dos valores sobre o Ordenador de Despesas, que deverá declarar a compatibilidade do preço da contratação com o preço de mercado à luz dos aspectos levantados.

Em derradeiro, extrai-se do Despacho que encaminhou o processo para análise jurídica de **Id. 1012518** as seguintes observações: *"Identifiquei que faltam assinaturas no ETP e mapa de riscos, além do ETP ter descrita a composição diferente do DFD; e a necessidade de ajuste no item referente a qualificação técnica que está sendo exigida, agrupando exigências pontuais de apresentação de documentos (atestados) e correção da numeração dos itens."* Cabe, portanto, ao setor responsável, a análise dos pontos ali levantados, em especial quanto à assinatura dos documentos eventualmente pendentes e a conferência do conteúdo do DFD com o do ETP. **[RECOMENDAÇÃO 03]**

III.C – DA ANÁLISE DE RISCOS

A Análise de Risco materializa-se no Mapa de Risco, conforme normatização da **Instrução Normativa nº 5, de 25 de maio de 2017**, artigos 25 ao 27.

A **análises de riscos** foi observada e inserida no **ID 0952056**, considerando as fases de planejamento da contratação e de seleção do fornecedor, respectivamente.

Verifica-se, no entanto, que até o momento, consta nos autos apenas a "Análise de Riscos", elaborado em etapa anterior à conclusão do Termo de

³ Acórdão nº 228/2002 – Plenário, rel. Min. Marcos Vinícios Vilaça, Processo nº 002.933/2001-8

⁴ 8.6.5 O que importa é que a eventual citação desses servidores não aproveitaria a defesa do recorrente, isso porque, como ordenador de despesa, deveria ter-se certificado acerca da regularidade da licitação, antes de formalizar o ato de homologação, o que não fez, pois atestou a regularidade do certame cujos preços estavam superfaturados, assumindo, desse modo, a responsabilidade solidária por tal irregularidade e, conseqüentemente, o risco de ser condenado, individualmente, a recolher o débito dela decorrente" (Acórdão nº 509/2005 – Plenário, rel. Min. Marcos Bemquerer Costa, Processo nº 775.051/1998-5).



Referência. Conforme previsto nos artigos 25 e 26 da IN SEGES nº 5/2017, o Gerenciamento de Riscos deve ser formalizado por meio do Mapa de Riscos, documento específico e estruturado que, inclusive, deve ser atualizado em momentos distintos do procedimento de contratação. Recomenda-se, portanto, a elaboração e juntada do referido Mapa de Riscos, em conformidade com o modelo indicado na referida Instrução Normativa, de modo a assegurar o adequado cumprimento das etapas previstas na gestão de riscos e conferir maior segurança ao processo. **[RECOMENDAÇÃO 04]**

III.D – DO TERMO DE REFERÊNCIA

Nota-se que a Comissão de Planejamento se valeu do TR para definição do objeto da licitação, conduta acertada considerando a natureza do objeto contratual – aquisição de bens. Como ensina MARÇAL JUSTEN FILHO, “o *Termo de Referência é exigido para a instauração de licitações e para contratações diretas para compras e serviços, que não configurem obra ou serviço de engenharia*”.⁵

O Termo de Referência está disciplinado no artigo 6º, XXIII, NLL, além da **Instrução Normativa SEGES/ME nº 81, de 25 de novembro de 2022**, cuja leitura e observância são obrigatórias no âmbito do CRCES.

Transcreve o conceito legal e os elementos constitutivos do Termo de Referência:

Art. 6º Para os fins desta Lei, consideram-se:

[...]

XXIII - termo de referência: documento necessário para a contratação de bens e serviços, que deve conter os seguintes parâmetros e elementos descritivos:

- a) definição do objeto**, incluídos sua natureza, os quantitativos, o prazo do contrato e, se for o caso, a possibilidade de sua prorrogação;
- b) fundamentação da contratação**, que consiste na referência aos estudos técnicos preliminares correspondentes ou, quando não for

⁵ JUSTEN FILHO, Marçal, Pedro. Comentários à Lei de Licitações e Contratos Administrativos: Lei 14.133/2021. São Paulo: Thomson Reuters Brasil, 2021, p. 175.



possível divulgar esses estudos, no extrato das partes que não contiverem informações sigilosas;

c) descrição da solução como um todo, considerado todo o ciclo de vida do objeto;

d) requisitos da contratação;

e) modelo de execução do objeto, que consiste na definição de como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento;

f) modelo de gestão do contrato, que descreve como a execução do objeto será acompanhada e fiscalizada pelo órgão ou entidade;

g) critérios de medição e de pagamento;

h) forma e critérios de seleção do fornecedor;

i) estimativas do valor da contratação, acompanhadas dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, com os parâmetros utilizados para a obtenção dos preços e para os respectivos cálculos, que devem constar de documento separado e classificado;

j) adequação orçamentária;

Primeiramente, dedicamo-nos aos comentários gerais sobre as cautelas do Administrador na especificação do objeto do futuro contrato.

Compete ao **Setor Requisitante** o ônus da **especificação do objeto** a ser licitado, o qual se responsabiliza por quaisquer restrições à ampla competitividade ou outra infração ao disposto na Lei nº 14.133/2021.

Assim, deve a área técnica verificar se nas especificações **não há exigências desnecessárias, irrelevantes ou desprovidas de critérios objetivos, que terminem por limitar a competição e/ou forçar a contratação com determinada empresa ou fornecedor**, ofendendo ao disposto nos arts. 5º e 9º, inciso I, alínea "a", da Lei nº 14.133/2021.

Logo, deverão ser tomadas as cautelas necessárias para assegurar que as **especificações correspondam àquelas essenciais ao bem**, sem as quais não poderão ser atendidas as necessidades do órgão, **evitando-se especificações que limitem a competição**.



O artigo 41 da Lei 14.133/2021 dispõe que, em caráter excepcional, a Administração poderá indicar ou vedar marca ou modelo de bens ou serviços, desde que observados requisitos específicos. Vejamos:

Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:

I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

- a) em decorrência da necessidade de padronização do objeto;
- b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;
- c) quando determinada marca ou modelo comercializados por mais de um fornecedor forem os únicos capazes de atender às necessidades do contratante;
- d) quando a descrição do objeto a ser licitado puder ser mais bem compreendida pela identificação de determinada marca ou determinado modelo aptos a servir apenas como referência;

[...]

III - vedar a contratação de marca ou produto, quando, mediante processo administrativo, restar comprovado que produtos adquiridos e utilizados anteriormente pela Administração não atendem a requisitos indispensáveis ao pleno adimplemento da obrigação contratual;

IV - solicitar, motivadamente, carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor.

Parágrafo único. A exigência prevista no inciso II do caput deste artigo restringir-se-á ao licitante provisoriamente vencedor quando realizada na fase de julgamento das propostas ou de lances

É fundamental que se tenha cautela redobrada quanto à indicação de marca ou modelo no procedimento licitatório. Isso porque tal medida exige, obrigatoriamente, justificativa prévia da necessidade, nos termos da norma legal.

Conforme o inciso I do Artigo 41, a excepcionalidade da indicação de marca ou modelo encontra respaldo apenas quando **houver processo formal de padronização, for necessária a compatibilidade com soluções já adotadas pela Administração ou restar comprovado que apenas determinada**



marca ou modelo, comercializada por mais de um fornecedor, é capaz de atender de forma adequada à necessidade administrativa, hipótese esta que deve estar necessariamente fundamentada no interesse público primário.

Destaca-se, ainda, que o processo de padronização, mencionado como uma das hipóteses legais de indicação de marca, está disciplinado no Art. 43 da Lei 14.133/2021, devendo, por razões lógicas e jurídicas, preceder à instauração do processo licitatório no qual a marca venha a ser indicada com base nesse fundamento.

Importa frisar que a jurisprudência do Tribunal de Contas da União já reconhece, há muito tempo, a possibilidade de adoção de procedimentos de padronização pela Administração Pública, desde que devidamente motivados e voltados à obtenção de soluções mais eficientes e vantajosas ao interesse público.

SÚMULA TCU 270: **Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação.**

Acórdão 849/2012-Plenário | Relator: JOSÉ MUCIO MONTEIRO

A indicação de marca no edital deve estar amparada em razões de ordem técnica, de forma motivada e documentada, que demonstrem ser aquela marca específica a única capaz de satisfazer o interesse público.

Acórdão 113/2016-Plenário | Relator: BRUNO DANTAS

Quanto à fundamentação da contratação **(item 2)**, nos termos do inciso XXIII, alínea "b", do dispositivo acima, o TR acertadamente faz referência ao Estudo Técnico Preliminar.

Apresentam-se, ademais, a descrição da solução e requisitos da contratação **(item 3)**, os requisitos da contratação e o modelo de execução do objeto **(item 4)**, critérios de medição e pagamento e adequação orçamentária **(item 7)** e forma e critérios de seleção de fornecedor **(item 8)**.

Quanto às estimativas do valor da contratação **(item 9)**, recomenda-se a menção expressa à Pesquisa de Preços e ao Mapa Comparativo de



Preços, em atendimento ao inciso XXIII, alínea "i", do art. 6º da Lei 14.133/21
[RECOMENDAÇÃO 05].

III.E – DA MINUTA DE CONTRATO.

A minuta de contrato NÃO é obrigatória em duas hipóteses:

Art. 95. O instrumento de contrato é obrigatório, salvo nas seguintes hipóteses, em que a Administração poderá substituí-lo por outro instrumento hábil, como carta-contrato, nota de empenho de despesa, autorização de compra ou ordem de execução de serviço:

I - dispensa de licitação em razão de valor;

II - compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto a assistência técnica, independentemente de seu valor.

Entrementes, nenhuma das duas situações excepcionais se faz presente no caso concreto.

A formalização do instrumento contratual que regulará as prestações de serviços artísticos de que trata este opinativo deve observar, no que cabe, às cláusulas necessárias aos contratos administrativos, conforme preleciona o art. 92 da Lei n. 14.133/2021:

Art. 92. São necessárias em todo contrato cláusulas que estabeleçam:

I - o objeto e seus elementos característicos;

II - a vinculação ao edital de licitação e à proposta do licitante vencedor ou ao ato que tiver autorizado a contratação direta e à respectiva proposta;

III - a legislação aplicável à execução do contrato, inclusive quanto aos casos omissos;

IV - o regime de execução ou a forma de fornecimento;

V - o preço e as condições de pagamento, os critérios, a data-base e a periodicidade do reajustamento de preços e os critérios de atualização monetária entre a data do adimplemento das obrigações e a do efetivo pagamento;



- VI** - os critérios e a periodicidade da medição, quando for o caso, e o prazo para liquidação e para pagamento;
- VII** - os prazos de início das etapas de execução, conclusão, entrega, observação e recebimento definitivo, quando for o caso;
- VIII** - o crédito pelo qual correrá a despesa, com a indicação da classificação funcional programática e da categoria econômica;
- IX** - a matriz de risco, quando for o caso;
- X** - o prazo para resposta ao pedido de repactuação de preços, quando for o caso;
- XI** - o prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, quando for o caso;
- XII** - as garantias oferecidas para assegurar sua plena execução, quando exigidas, inclusive as que forem oferecidas pelo contratado no caso de antecipação de valores a título de pagamento;
- XIII** - o prazo de garantia mínima do objeto, observados os prazos mínimos estabelecidos nesta Lei e nas normas técnicas aplicáveis, e as condições de manutenção e assistência técnica, quando for o caso;
- XIV** - os direitos e as responsabilidades das partes, as penalidades cabíveis e os valores das multas e suas bases de cálculo;
- XV** - as condições de importação e a data e a taxa de câmbio para conversão, quando for o caso;
- XVI** - a obrigação do contratado de manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação na licitação, ou para a qualificação, na contratação direta;
- XVII** - a obrigação de o contratado cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;
- XVIII** - o modelo de gestão do contrato, observados os requisitos definidos em regulamento;
- XIX** - os casos de extinção.

Em relação aos termos da minuta, verificamos que esta observa, no que cabe, às cláusulas necessárias aos contratos administrativos, conforme preleciona o aludido artigo 92 da Nova Lei de Licitações.

III.F – DO EDITAL



Traçadas essas premissas e demonstrada a adequação do procedimento administrativo até o presente, passa-se, neste momento, à análise jurídica da Minuta de Edital (**ID 1012514**).

O conteúdo do Edital está previsto no **artigo 25** e o procedimento eletrônico está regulamentado na **Instrução Normativa SEGES nº 73, de 30 de setembro de 2022**⁶. Veja-se o art. 25 do mencionado diploma legal:

Art. 25. O edital deverá conter o **objeto da licitação** e as regras relativas à **convocação**, ao **julgamento**, à **habilitação**, aos **recursos** e às **penalidades** da licitação, à **fiscalização** e à **gestão do contrato**, à **entrega do objeto** e às **condições de pagamento**.

(...)

§ 7º Independentemente do prazo de duração do contrato, será obrigatória a previsão no edital de índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado e com a possibilidade de ser estabelecido mais de um índice específico ou setorial, em conformidade com a realidade de mercado dos respectivos insumos.

§ 8º Nas licitações de serviços contínuos, observado o interregno mínimo de 1 (um) ano, o critério de reajustamento será por:

I - reajustamento em sentido estrito, quando não houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante previsão de índices específicos ou setoriais;

II - repactuação, quando houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

A **elaboração de Edital de Licitação** atende ao requisito do art. 18, V, e ainda, apresenta todo o conteúdo obrigatório que está disciplinado no artigo 25 e em outros artigos esparsos da Lei nº 14.133/21, além da abordagem de temas dispostos em razão de outros incisos do artigo 18 (III, VII e VIII).

Analisando a Minuta de Edital, verificamos que todos os itens descritos no *caput* do art. 25 da lei acima citada são abordados por meio do uso de nomes similares de capítulos específicos do Edital, o que demonstra que todo o conteúdo fora tratado.

⁶ Essa IN SEGES disciplina o procedimento licitatório eletrônico para as modalidades de pregão, concorrência e para a fase competitiva do diálogo competitivo, quando “for entendido como o mais adequado à solução identificada na fase de diálogo.



Ao que se percebe, tratou-se de técnica de construção que já é adotada pela AGU para evitar a reprodução do mesmo conteúdo em documentos que estão anexados, a fim de tornar mais concisa e objetiva a materialização do planejamento da contratação.

IV. CONCLUSÃO:

Assim, ante o exposto, opina-se pela viabilidade jurídica da deflagração do procedimento licitatório na modalidade pregão, na forma eletrônico, **desde que cumpridas as recomendações constantes neste parecer.**

É o opinativo.

Vitória/ES, 16 de Setembro de 2025.

IGOR OLIVEIRA DE
MORAES  Assinado de forma digital por
IGOR OLIVEIRA DE
MORAES 
Dados: 2025.09.16 10:26:07 -03'00'

IGOR OLIVEIRA DE MORAES
Ribeiro Fialho Advogados
Advogado - 



ESTUDO TÉCNICO PRELIMINAR

Processo nº 9079618110000798.000048/2025-57

ESTUDOS PRELIMINARES

O presente documento visa analisar a viabilidade da presente contratação, bem como levantar os elementos essenciais que servirão para compor o Termo de Referência ou projeto Básico, de forma a melhor atender às necessidades da Administração.

Dados do Processo:

Órgão Responsável pela Contratação:	Conselho Regional de Contabilidade do Espírito Santo.
Objeto:	Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
Nº do Processo Administrativo:	9079618110000798.000048/2025-57

1. Justificativa para a Contratação Conjunta de Serviços de Tecnologia da Informação:**1.1. Introdução**

O presente estudo tem como objetivo fundamental apresentar a justificativa técnica e legal para a contratação conjunta de diversos serviços de Tecnologia da Informação (TI) pelo Conselho Regional de Contabilidade do Espírito Santo (CRCES). A decisão por uma contratação unificada, em detrimento da fragmentação em múltiplos contratos, fundamenta-se em princípios basilares da administração pública, notadamente a economicidade, a eficiência, a segurança jurídica e a busca pela solução mais vantajosa para a Administração, em consonância com as diretrizes estabelecidas pela Lei nº 14.133/21.

A infraestrutura de TI do CRCES, conforme detalhado ao longo deste documento, é um pilar essencial para a continuidade e a qualidade dos serviços prestados à sociedade e à classe contábil. A complexidade e a interdependência dos serviços de Wi-Fi corporativo, backup, suporte técnico e firewall demandam uma abordagem integrada para garantir a robustez, a segurança e a disponibilidade dos sistemas críticos. A contratação isolada de cada um desses componentes não apenas eleva os riscos operacionais, mas também compromete a gestão eficiente e a otimização dos recursos públicos.

Este texto abordará os aspectos técnicos e jurídicos que sustentam a opção pela contratação conjunta, destacando os benefícios em termos de economicidade, a mitigação de problemas inerentes à multiplicidade de prestadores de serviços e a conformidade com a legislação vigente, em especial a Lei nº 14.133/2021 e as melhores práticas de contratação de soluções de TI para a Administração Pública.

1.2. Da Necessidade da Contratação e a Interdependência dos Serviços de TI

O Conselho Regional de Contabilidade do Espírito Santo (CRCES) reconhece a Tecnologia da Informação como um elemento estratégico e indispensável para o cumprimento de sua missão institucional. A atual infraestrutura de TI, embora funcional, enfrenta desafios significativos que justificam a presente contratação. Conforme o documento de Estudos Preliminares, o CRCES dispõe de apenas um funcionário técnico especializado em TI, o que resulta em sobrecarga de trabalho e na impossibilidade de atender a todas as demandas operacionais e administrativas complexas, como a manutenção de servidores, gestão de incidentes, monitoramento contínuo de redes, implementação de políticas de segurança da informação e suporte técnico especializado. Adicionalmente, a rede cabeada existente apresenta falhas que impactam diretamente a conectividade e a produtividade da instituição.

A contratação em questão visa suprir essas lacunas e fortalecer a infraestrutura de TI do CRCES, abrangendo os seguintes serviços essenciais e interdependentes:

• **Solução de Acesso via Wi-Fi:** Fundamental para garantir conectividade de alta qualidade e superar as limitações da rede cabeada atual,

promovendo a mobilidade e a eficiência no ambiente de trabalho.

•**Firewall de Próxima Geração:** Crucial para fortalecer a segurança da rede, proteger os dados do CRCES contra ameaças cibernéticas e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

•**Serviços Continuados de Suporte (N1, N2 e N3):** Essenciais para a manutenção da infraestrutura tecnológica, garantia do funcionamento adequado dos sistemas críticos, gestão de incidentes e mudanças, e monitoramento contínuo da infraestrutura.

•**Backup Corporativo (Local e em Nuvem):** Indispensável para assegurar a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, garantindo a continuidade dos negócios e a conformidade com a LGPD.

A natureza desses serviços é intrinsecamente interligada. A eficácia de um sistema de backup, por exemplo, depende diretamente da segurança da rede (Firewall) e da capacidade de suporte técnico para gerenciar eventuais falhas. Da mesma forma, a qualidade da conectividade Wi-Fi impacta a performance de todas as aplicações e serviços que trafegam pela rede. A contratação fragmentada desses serviços, com diferentes prestadores, geraria uma série de desafios e riscos que serão detalhados nas seções seguintes, comprometendo a eficiência e a segurança da infraestrutura de TI do CRCES.

1.3. Arcabouço Legal: A Lei nº 14.133/2021 e os Princípios da Contratação Pública

A Nova Lei de Licitações e Contratos Administrativos, Lei nº 14.133, de 1º de abril de 2021, trouxe inovações significativas para o processo de contratação pública no Brasil, com o objetivo de modernizar, otimizar e tornar mais eficientes as aquisições e contratações realizadas pela Administração Pública. Em seu Art. 5º, a Lei elenca uma série de princípios que devem nortear a aplicação da norma, dentre os quais se destacam a economicidade, a eficiência, o interesse público, o planejamento, a transparência, a segurança jurídica e a vantajosidade. Estes princípios são pilares para a justificativa da contratação conjunta dos serviços de TI.

A Lei nº 14.133/2021, ao contrário da legislação anterior, enfatiza a busca pela solução mais vantajosa para a Administração, que não se restringe apenas ao menor preço, mas considera a relação custo-benefício, a qualidade, a inovação e a sustentabilidade. A contratação conjunta de serviços de TI, quando devidamente justificada, alinha-se perfeitamente a essa premissa, pois permite uma visão sistêmica e integrada da infraestrutura, otimizando recursos e minimizando riscos.

Embora a Lei nº 14.133/2021 defina a 'contratação integrada' especificamente para obras e serviços de engenharia (Art. 6º, XXXII), o conceito subjacente de agrupar itens interdependentes para obter maior eficiência e vantajosidade pode ser analogicamente aplicado à contratação de serviços de TI. A Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que disciplina as contratações de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades do SISP, reforça a importância do planejamento e da busca por soluções que atendam às necessidades de forma abrangente e eficiente.

O Estudo Técnico Preliminar (ETP), conforme previsto na Lei nº 14.133/2021 e detalhado na IN SGD/ME Nº 94/2022, é o documento fundamental que embasa a decisão pela contratação. Ele deve contemplar a análise comparativa de soluções e custos, a estimativa do custo total da

contratação e a declaração da viabilidade da contratação. A presente justificativa, ao demonstrar os benefícios da contratação conjunta, serve como subsídio para o ETP, evidenciando que a opção por um único prestador para os serviços de Wi-Fi, backup, suporte e firewall é a que melhor atende aos princípios da Lei e às necessidades do CRCES.

Outro ponto relevante é a Matriz de Alocação de Riscos, que se torna ainda mais crucial em contratações complexas como a de serviços de TI. A Lei nº 14.133/2021 exige a definição clara de riscos e responsabilidades entre as partes. Em uma contratação conjunta, a alocação de riscos é simplificada, pois a responsabilidade pela integração e funcionamento dos diversos componentes recai sobre um único fornecedor, facilitando a gestão e a resolução de eventuais problemas.

1.4. Economicidade e Vantagens da Contratação Conjunta

A busca pela economicidade é um dos princípios fundamentais que regem as contratações públicas, conforme expresso no Art. 5º da Lei nº 14.133/2021. A contratação conjunta dos serviços de TI, em vez de licitações separadas para cada item (Wi-Fi, backup, suporte e firewall), representa uma estratégia que maximiza a eficiência na aplicação dos recursos públicos e gera uma série de vantagens econômicas e operacionais para o CRCES.

Primeiramente, a contratação de um único fornecedor para a gestão integrada de múltiplos serviços de TI permite a obtenção de economias de escala. Ao consolidar a demanda, o CRCES ganha maior poder de negociação, o que pode resultar em propostas mais competitivas e preços unitários mais vantajosos para cada serviço. A diluição de custos administrativos e operacionais do fornecedor em um contrato de maior escopo tende a refletir em um custo total da contratação mais baixo para a Administração Pública.

Além disso, a contratação conjunta simplifica os processos administrativos e burocráticos. A gestão de um único contrato, em comparação com a gestão de múltiplos contratos, reduz significativamente a carga de trabalho da equipe interna do CRCES, liberando recursos humanos para outras atividades estratégicas. Isso se traduz em economia de tempo e, consequentemente, de recursos financeiros, uma vez que menos horas de trabalho são dedicadas à fiscalização e acompanhamento de diversos contratos.

A otimização dos recursos também se manifesta na redução de custos indiretos. A coordenação entre diferentes fornecedores, a resolução de conflitos de responsabilidade e a necessidade de interface entre sistemas distintos geram custos ocultos e ineficiências. Com um único prestador, esses custos são minimizados, pois a responsabilidade pela integração e pelo funcionamento harmonioso de toda a infraestrutura de TI recai sobre uma única empresa, que possui o conhecimento global do ambiente e a capacidade de gerenciar as interdependências de forma proativa.

Por fim, a contratação conjunta contribui para a previsibilidade orçamentária. Com um contrato abrangente, o CRCES tem uma visão mais clara e consolidada dos custos totais envolvidos na manutenção e gestão de sua infraestrutura de TI, facilitando o planejamento financeiro e a alocação de recursos de forma mais eficiente ao longo do tempo. Essa previsibilidade é essencial para uma gestão pública responsável e transparente.

1.5. Mitigação de Problemas e Impactos Negativos da Multiplicidade de Prestadores

A contratação fragmentada de serviços de Tecnologia da Informação, com a pulverização de responsabilidades entre múltiplos prestadores, embora possa parecer, à primeira vista, uma estratégia de diversificação, acarreta uma série de problemas e impactos negativos que comprometem a eficiência, a segurança e a continuidade das operações do CRCES. A experiência demonstra que a gestão de diversos contratos para serviços interdependentes de TI pode gerar complexidades e vulnerabilidades que superam quaisquer supostas vantagens.

Um dos principais desafios reside na incompatibilidade e nas falhas de integração entre os diferentes sistemas e equipamentos fornecidos por empresas distintas. A infraestrutura de TI do CRCES, conforme descrito, é híbrida e complexa, envolvendo soluções de Wi-Fi, backup, suporte e firewall, além de infraestrutura hiperconvergente, acessos VDI, máquinas virtuais e desktops físicos. A falta de um gerenciamento unificado pode levar a problemas de interoperabilidade, dificultando a comunicação entre os componentes e resultando em falhas operacionais, interrupções de serviço e degradação da performance geral do ambiente. A identificação da causa raiz de um problema torna-se um processo moroso e dispendioso, pois cada fornecedor pode atribuir a falha ao outro, criando um cenário de “empurra-empurra” de responsabilidades.

A dificuldade na gestão e fiscalização contratual é outro impacto negativo significativo. A multiplicidade de contratos implica na necessidade de gerenciar diferentes prazos, escopos, níveis de serviço (SLAs) e pontos de contato. Isso sobrecarrega a equipe interna do CRCES, que já é reduzida, desviando seu foco de atividades estratégicas para a burocracia administrativa. A fiscalização torna-se mais complexa, exigindo um esforço desproporcional para garantir que cada fornecedor esteja cumprindo suas obrigações de forma isolada, sem uma visão integrada do impacto no ambiente como um todo.

A diluição da responsabilidade é um risco inerente à contratação fragmentada. Em caso de incidentes de segurança, falhas de sistema ou perda de dados, a apuração do responsável pela falha e a consequente aplicação de sanções contratuais tornam-se extremamente difíceis. Essa incerteza jurídica pode atrasar a resolução de problemas críticos, gerar prejuízos financeiros e de imagem para o CRCES, e comprometer a conformidade com regulamentações como a LGPD. Com um único prestador, a responsabilidade pela integridade e funcionamento de toda a infraestrutura é centralizada, facilitando a governança e a responsabilização.

Adicionalmente, a fragmentação pode levar a custos elevados e ineficiências operacionais. A ausência de uma visão consolidada da infraestrutura impede a otimização de recursos e a identificação de redundâncias ou gargalos. Cada fornecedor pode operar de forma isolada, sem considerar o impacto de suas ações no ambiente geral, o que pode resultar em investimentos desnecessários ou na subutilização de ativos. A falta de padronização e a necessidade de múltiplas interfaces de comunicação entre os fornecedores também contribuem para o aumento dos custos operacionais.

Por fim, a vulnerabilidade de segurança é amplificada em um ambiente com múltiplos prestadores. A gestão de segurança da informação exige uma abordagem holística e integrada. A fragmentação pode criar brechas e pontos cegos, dificultando a implementação de políticas de segurança consistentes e a resposta rápida a ameaças cibernéticas. Um único fornecedor, com uma visão abrangente da infraestrutura, está em melhor posição para implementar e gerenciar soluções de segurança de forma eficaz, garantindo a proteção dos dados e sistemas do CRCES.

Diante desses riscos e impactos negativos, a contratação conjunta de serviços de TI emerge como a solução mais prudente e vantajosa para o CRCES, garantindo a sinergia entre os serviços, a otimização da gestão, a clareza na alocação de responsabilidades e a segurança da infraestrutura tecnológica.

1.6. Conclusão

Diante do exposto, a contratação conjunta dos serviços de Tecnologia da Informação para o Conselho Regional de Contabilidade do Espírito Santo (CRCES), abrangendo Wi-Fi corporativo, backup, serviços de suporte e firewall, configura-se como a abordagem mais estratégica, eficiente e em conformidade com os preceitos da Lei nº 14.133/2021. Esta modalidade de contratação não apenas otimiza a aplicação dos recursos públicos, mas também mitiga os riscos inerentes à fragmentação de serviços interdependentes, garantindo a continuidade, a segurança e a qualidade da infraestrutura de TI do órgão.

A centralização da responsabilidade em um único prestador de serviços especializados em TI proporciona uma gestão mais simplificada e eficaz, com clareza na alocação de responsabilidades e maior agilidade na resolução de problemas. A economicidade é alcançada por meio de ganhos de escala, redução de custos administrativos e operacionais, e maior previsibilidade orçamentária. Adicionalmente, a abordagem integrada fortalece a segurança da informação, minimizando vulnerabilidades e garantindo a conformidade com a legislação vigente, como a LGPD.

Em suma, a contratação conjunta é a solução que melhor atende ao interesse público, promovendo a eficiência, a economicidade e a segurança jurídica, pilares da boa gestão pública. Recomenda-se, portanto, a continuidade do processo licitatório sob esta perspectiva integrada, visando a obtenção da proposta mais vantajosa e a garantia de uma infraestrutura de TI robusta e confiável para o CRCES.

2. Diretrizes gerais para a contratação:

2.1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERADO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INT PÙBLICO;

O **Conselho Regional de Contabilidade do Espírito Santo (CRCES)** desempenha um papel essencial na sociedade, oferecendo serviços como fiscalização e registro do exercício profissional, orientação técnica e promoção de desenvolvimento profissional da classe contábil. A execução eficiente dessas atividades depende diretamente de uma **infraestrutura de Tecnologia da Informação (TI)** robusta, segura e eficaz, capaz de atender às crescentes demandas internas e externas e garantir a proteção de dados sensíveis, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**.

Atualmente, o CRCES conta com apenas **um servidor técnico especializado em TI**, o qual se encontra sobrecarregado com demandas operacionais, administrativas e técnicas. Essa limitação compromete a execução de atividades críticas e complexas, como:

- Manutenção de servidores e redes;
- Monitoramento contínuo da infraestrutura;
- Gestão de incidentes e mudanças;
- Suporte técnico especializado;
- Implementação de políticas de segurança da informação.

Além disso, a **infraestrutura de rede cabeada apresenta falhas recorrentes**, impactando diretamente a conectividade e a produtividade das equipes. A segurança da informação também requer reforços, com a **adoção de soluções modernas e eficazes contra ameaças cibernéticas**.

Atualmente, o CRCES mantém o **Contrato Administrativo nº 40/2024**, firmado com a empresa Smart Fusion Technology Ltda, com vigência até 15/12/2025. Contudo, trata-se de contrato emergencial, **sem possibilidade de prorrogação**, o que torna **necessária a realização de novo procedimento licitatório**, a fim de garantir a contratação regular e contínua dos serviços especializados de gerenciamento de TI.

A nova contratação tem como objetivo **assegurar a continuidade, eficiência e segurança das operações tecnológicas do CRCES**, por meio da prestação dos seguintes serviços especializados:

- Suporte técnico avançado para a infraestrutura tecnológica;
- Manutenção preventiva e corretiva de servidores e redes;
- Gestão de incidentes e implementação de melhorias;
- Monitoramento proativo da infraestrutura de TI;

- Fornecimento, instalação e gestão de **rede Wi-Fi corporativa**;
- Implantação e gestão de **Firewall de Próxima Geração**;
- Implementação e gerenciamento de **solução de backup híbrida** (local e em nuvem), conforme exigências da LGPD.

Além disso, a contratação visa **reduzir a sobrecarga do único servidor de TI**, promovendo maior eficiência e qualidade dos serviços prestados pelo Conselho à sociedade e à classe contábil.

Natureza do Objeto – Serviço Comum e Continuado

O objeto desta contratação caracteriza-se como **serviço comum**, nos termos do inciso II do art. 6º da **Lei nº 14.133/2021**, por poder ser descrito de forma objetiva e padronizada, sem necessidade de especificações técnicas complexas ou qualificações exclusivas. São serviços amplamente ofertados no mercado, com condições técnicas e comerciais similares entre fornecedores.

Trata-se, ainda, de **serviço de natureza continuada**, tendo em vista a sua **necessidade permanente e ininterrupta**, indispensável à execução das atividades finalísticas do CRCES. A descontinuidade desses serviços comprometeria a segurança da informação, a funcionalidade dos sistemas internos e a continuidade do atendimento ao público.

Diante do exposto, justifica-se a abertura de procedimento licitatório para a **contratação regular de serviços comuns e continuados de gerenciamento de TI**, garantindo:

- A continuidade das atividades institucionais do CRCES;
- A observância aos princípios da legalidade, eficiência e economicidade;
- A proteção de dados sensíveis, conforme previsto na LGPD;
- A segurança, estabilidade e evolução da infraestrutura tecnológica do Conselho

2.1.1 – JUSTIFICATIVA PARA CONTRATAÇÃO CONJUNTA DOS SERVIÇOS

2.2 - PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

A contratação possui previsão no Plano de Contratações Anual do CRCES para o exercício 2026, e no Plano Diretor de Tecnologia da Informação.

2.3 - REQUISITOS DA CONTRATAÇÃO

		ITEM 1			
SUBITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

2.3.1 A Contratada deverá prestar **serviços gerenciados de Tecnologia da Informação** que abrangem o **suporte técnico avançado** (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a **gestão de incidentes e mudanças**. O escopo prevê a **gestão completa da infraestrutura de redes** (LAN, VLAN e WLAN), com o **fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa**, e a **gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais**. Será responsável também pelo **monitoramento contínuo da infraestrutura**, com identificação e mitigação proativa de riscos, pela **manutenção preventiva e corretiva** de todo o parque de TI, pela **gestão e monitoramento dos links de internet**, pela **gestão e manutenção da infraestrutura hiperconvergente** e do **banco de dados em SQL Server**. Além disso, inclui o **fornecimento, instalação e gestão de um Firewall de Próxima Geração** e a **implementação e gestão de solução de backup local e em nuvem**. Os serviços atenderão a única localidade do CRCES, até **60 estações de trabalho** (físicas ou virtuais), **5 servidores físicos** e **12 servidores virtuais**.

2.3.2 A empresa contratada deverá estar plenamente capacitada para **gerenciar toda a estrutura de TI híbrida do CRCES**. Esta estrutura é complexa e inclui uma infraestrutura hiperconvergente (sem armazenamento baseado em Software-defined Storage - SDS), uma infraestrutura

complexa e inclui uma **infraestrutura hiperconvergente** (com armazenamento baseado em software-defined storage - SDS), uma **infraestrutura com acessos VDI (Virtual Desktop Infrastructure)** máquinas virtuais e uma **infraestrutura tradicional** (com desktops físicos e notebooks). A Contratada será responsável por assegurar a **gestão completa dos backups e restores** de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a **disponibilidade e integridade dos dados** em todas as plataformas.

2.4 CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS

2.4.1. SOLUÇÃO DE ACESSO VIA WI-FI.

2.4.1.1. Características da solução.

2.4.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

2.4.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

2.4.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

2.4.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

2.4.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

2.4.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

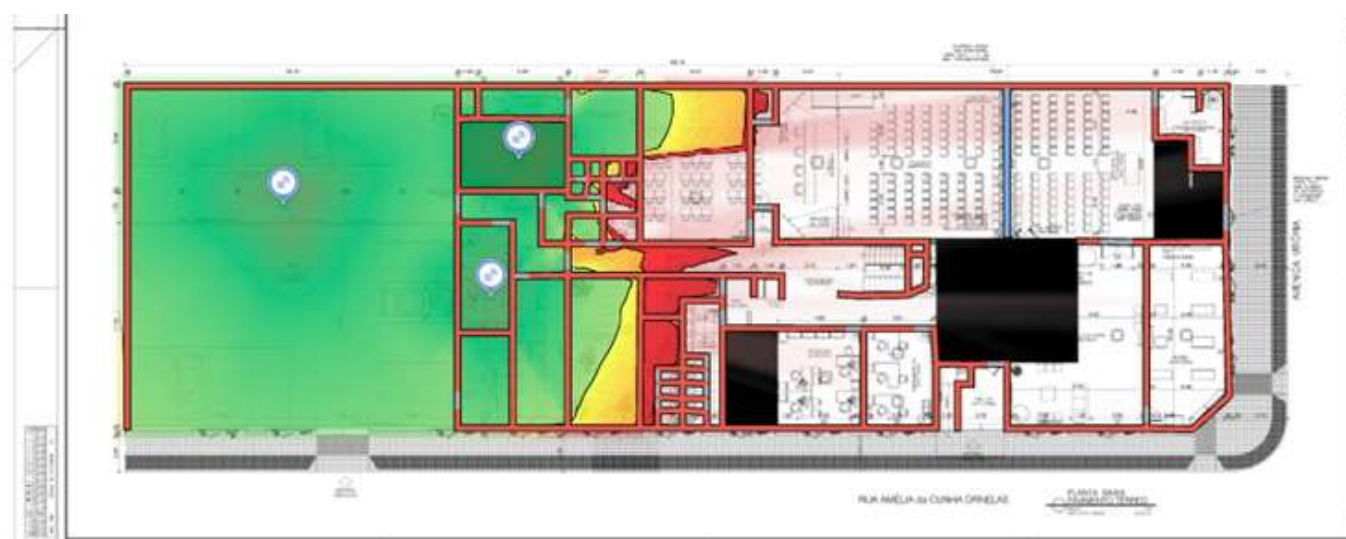
2.4.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.4.1.1.8. Site Survey Preliminar

Para a definição da quantidade de **equipamentos** necessários, conforme detalhado no item 2.4.1.1.2, o CRCES realizou um **levantamento de campo (site survey)** preliminar, cujos resultados são apresentados a seguir:

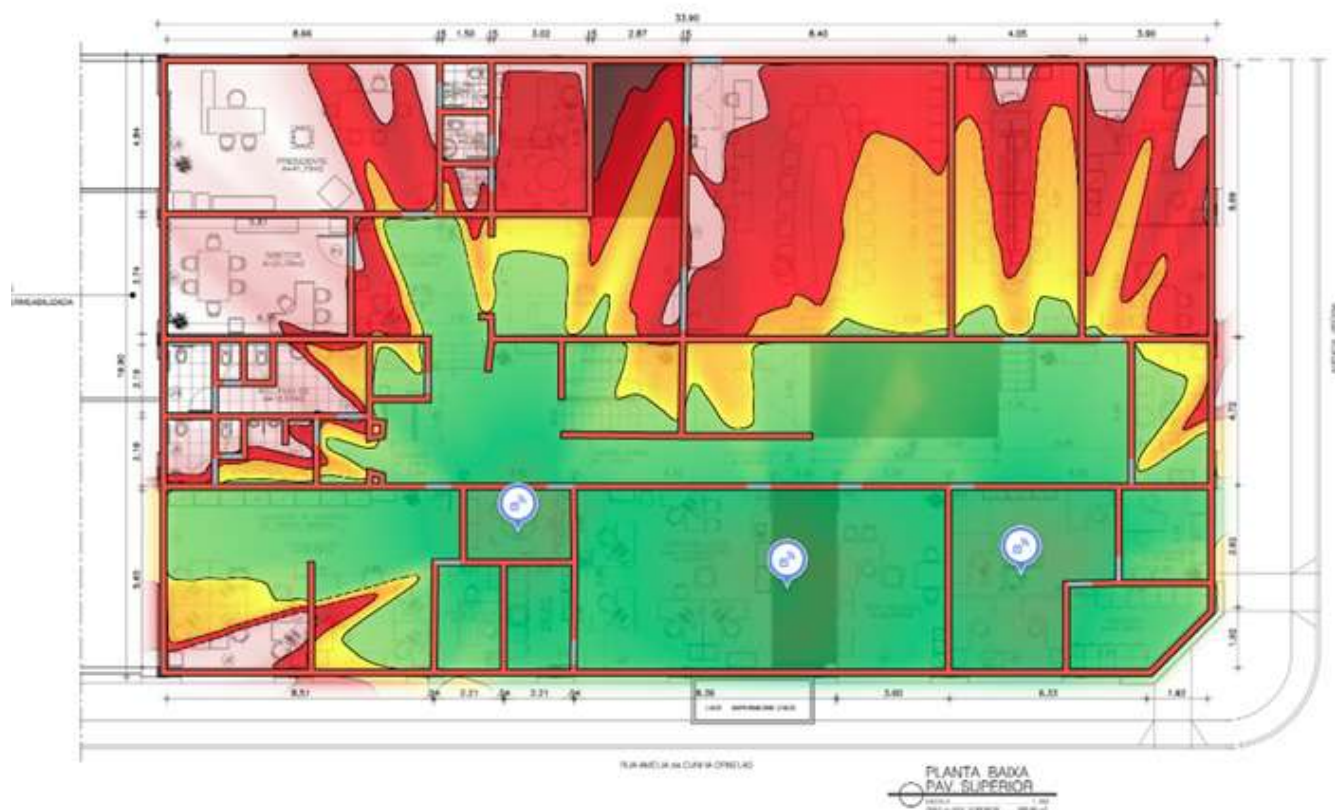
a) Pavimento térreo - 09 equipamentos





b) Pavimento superior - 09 equipamentos







2.5 CARACTERÍSTICAS DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.

2.5.1. Características dos pontos de acesso à internet via Wifi. (Equivalente ao seu antigo 1.2)

2.5.1.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

2.5.1.2. Deve ser compatível e gerenciado pelo ITENS "Firewall de Próxima Geração (NGFW) – Tipo 0x" deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

2.5.1.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

2.5.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

2.5.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

2.5.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

2.5.1.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

2.5.1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

2.5.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

2.5.1.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

2.5.1.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

2.5.1.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

2.5.1.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power

Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

2.5.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

2.5.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

2.5.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.5.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.5.1.20. Deve permitir operação em modo Mesh;

2.5.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

2.5.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

2.5.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

2.5.1.24. Deve suportar OFDMA;

2.5.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;

2.5.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

2.5.1.27. Deve suportar BSS Coloring;

2.5.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

2.5.1.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;

2.5.1.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);

2.5.1.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;

2.5.1.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;

2.5.1.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

2.5.1.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.5.1.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

2.5.1.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

2.5.1.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);

2.5.1.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

2.5.1.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

2.5.1.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

2.5.1.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.5.1.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.5.1.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.5.1.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.5.1.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.5.1.46. Deve implementar o padrão IEEE 802.11e;

2.5.1.47. Deve implementar o padrão IEEE 802.11h;

2.5.1.48. Deve implementar o padrão IEEE 802.3az;

2.5.1.49. Deve suportar ser gerenciado via SNMP;

2.5.1.50. Deve suportar consultas via REST API;

2.5.1.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

2.5.1.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;

2.5.1.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

2.5.1.54. Deve possuir indicadores luminosos (LED) para indicação de status;

2.5.1.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

2.5.1.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

2.5.1.57. Deve possuir certificado emitido pela Wi-Fi Alliance;

2.5.1.58. Deve estar homologado pela ANATEL na data de execução do pregão;

2.5.1.59. Deve ser licenciado para uso pelo período de duração da contratação.

2.5.1.60. Deve possuir garantia para uso pelo período de duração da contratação.

2.5.1.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

2.6. CARACTERÍSTICAS DO EQUIPAMENTO CONTROLADOR DE PONTOS DE ACESSO WIFI

2.6.1. Características do equipamento controlador de pontos de acesso Wifi (Equivalente ao seu antigo 1.3)

2.6.1.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

2.6.1.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

2.6.1.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

2.6.1.4. Deverá implementar os padrões IEEE 802.3af (PoE) e IEEE 802.3at (PoE+) com PoE budget de 370W em 24 portas;

2.6.1.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

2.6.1.6. Deve possuir 1 (uma) interface USB;

2.6.1.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);

2.6.1.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

2.6.1.9. Deve possuir tabela MAC com suporte a 32.000 endereços;

2.6.1.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

2.6.1.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

2.6.1.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (LACP);

2.6.1.13. Deve suportar a comutação de Jumbo Frames;

2.6.1.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

2.6.1.15. Deve implementar roteamento (camada 3) do modelo OSI entre as VLANs;

2.6.1.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

2.6.1.17. Deve implementar serviço de DHCP Relay;

2.6.1.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

2.6.1.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

2.6.1.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (RSTP) e IEEE 802.1s (MST). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

2.6.1.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

2.6.1.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

2.6.1.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

2.6.1.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

2.6.1.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

2.6.1.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

2.6.1.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

2.6.1.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

2.6.1.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

2.6.1.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

2.6.1.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

2.6.1.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

2.6.1.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

2.6.1.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

2.6.1.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

2.6.1.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

2.6.1.37. Deve suportar MAC Authentication Bypass (MAB);

2.6.1.38. Deve implementar RADIUS CoA (Change of Authorization);

2.6.1.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

2.6.1.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

2.6.1.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

2.6.1.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

2.6.1.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

2.6.1.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

2.6.1.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

2.6.1.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

2.6.1.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

2.6.1.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

2.6.1.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

2.6.1.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

2.6.1.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

2.6.1.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

- 2.6.1.53. Deve permitir ser gerenciado através de IPv6;
- 2.6.1.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 2.6.1.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 2.6.1.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 2.6.1.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 2.6.1.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 2.6.1.59. Deverá suportar ser configurado e monitorado através de REST API;
- 2.6.1.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 2.6.1.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 2.6.1.62. Deve suportar temperatura de operação de até 45º Celsius;
- 2.6.1.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 2.6.1.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 2.6.1.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 2.6.1.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 2.6.1.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 2.6.1.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

2.7 REQUISITOS DA INSTALAÇÃO DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.

- 2.7.1. Requisitos para instalação do item 1.2
- 2.7.2. Serviço de Implementação para rede WLAN
- 2.7.3. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura total, sendo observada a quantidade mínima estabelecida pela DTIC.
- 2.7.4. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;
- 2.7.5. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;
- 2.7.6. Requisitos gerais de Implantação
- 2.7.7. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.
- 2.7.8. Instalação física
- 2.7.9. Será realizada instalação física conforme a necessidade da contratante.
- 2.7.10. O ponto de acesso wifi deverá ser fixado no teto ou parede.
- 2.7.11. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

2.8 IMPLEMENTAÇÃO LÓGICA

- 2.8.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir
- 2.8.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.
- 2.8.3. Cadastro das subscrições dos APs na plataforma de gerência;
- 2.8.4. Endereçamento e segmentação das Redes WIRELESS;
- 2.8.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless);
- 2.8.6. Definição de políticas de bloqueio e permissão de acesso;
- 2.8.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 2.8.8. Configuração de Endereços/Interfaces de Gerência:
- 2.8.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 2.8.10. Parâmetros SNMP para monitoração/gerência remota;
- 2.8.11. Configuração de Syslog, quando aplicável;
- 2.8.12. Configuração de redes locais (VLANs);
- 2.8.13. Configuração de redes locais (SSIDs);
- 2.8.14. Configuração de sincronismo de hora NTP ou SNTP;
- 2.8.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 2.8.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 2.8.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 2.8.18. Configurações de grupos de ponto de acesso;
- 2.8.19. Configuração de algoritmo de criptografia a ser utilizado;
- 2.8.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 2.8.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 2.8.22. Configuração de segurança de rede;
- 2.8.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 2.8.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 2.8.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;

2.8.26. Emissão de relatórios de implantação contendo:

2.8.27. Mapas de rede,

2.8.28. Relação de equipamentos implantados,

2.8.29. Configurações feitas nos softwares;

2.8.30. Resultado dos testes realizados;

2.9 REQUISITOS PARA INSTALAÇÃO DO CONTROLADOR DE PONTOS DE ACESSO WIFI

2.9.1. Todo o processo de instalação será precedido de um estudo e entendimento de toda a infraestrutura em funcionamento hoje no ambiente englobando sua topologia, todas as configurações em uso (endereçamentos IP, VLANs, rotas, QoS, ACL's, etc),

2.9.2. Para a implementação da solução bem como acompanhamento do projeto proposto, a licitante deverá apresentar profissionais certificados, níveis avançados de conhecimento nas tecnologias ofertadas e necessárias para implantação da solução proposta.

2.9.3. O serviço de instalação, configuração da rede precederá de um cronograma de projeto para implementação das ações abaixo descritas, a ser elaborado de comum acordo.

2.9.4. Todo serviço deverá ser realizado por profissional do fabricante ou certificado por ele para execução dos serviços, para isso deverá ser apresentado junto com a proposta o certificado do profissional que irá executar os serviços de implantação

2.9.5. Planejamento e Projeto para Instalação da Solução

2.9.6. Levantamento e análise da configuração atual da rede;

2.9.7. Elaboração de Projeto de Rede detalhado em conjunto com a equipe de tecnologia da informação, incluindo os itens de configuração a seguir:

2.9.8. Endereçamento e segmentação das Redes LAN e WAN;

2.9.9. Roteamento estativo e dinâmico utilizando protocolos RIPv2 e OSPFv2, se aplicável;

2.9.10. Qualidade de Serviço (QoS): regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede;

2.9.11. Segurança:

2.9.12. Dos ativos: protocolos de comunicação segura, autenticação para acesso e proteção contra ataques;

2.9.13. Da rede: controles a serem implementados para restringir o acesso à rede e reduzir a exposição dos servidores e estações de trabalho;

2.9.14. Instalação da Solução

2.9.15. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;

2.9.16. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

2.9.17. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;

2.9.18. Configuração de Endereços/Interfaces de Gerência;

2.9.19. Endereçamento IP;

2.9.20. Telnet, se necessário;

2.9.21. Secure Shell (SSH), se necessário;

2.9.22. Web (HTTP), se necessário;

2.9.23. Restrições (Filtros/ACLs) de Acesso;

2.9.24. Autenticação;

2.9.25. Parâmetros SNMP para monitoração/gerência remota;

2.9.26. Configuração de redes locais (VLANs);

2.9.27. Configuração de sincronismo de hora NTP ou SNTP;

2.9.28. Configuração do protocolo Rapid Spanning Tree (RSTP);

2.9.29. Configuração de BPDU GUARD;

2.9.30. Configuração de Root Spanning Tree;

2.9.31. Interfaces de roteamento IP;

2.9.32. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;

2.9.33. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;

2.9.34. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.35. Otimização da Solução

2.9.36. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

2.9.37. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.38. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;

2.9.39. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto

2.9.40. Ativação de recursos para o controle de broadcast storms;

2.9.41. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.42. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.43. Controle de acesso a rede através do padrão IEEE 802.1x;

2.9.44. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;

2.9.45. Configuração de DHCP Snooping;

2.9.46. Configuração de DHCP Relay;

2.9.47. Configuração de interface confiável (trust Interface);

2.9.48. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.

2.9.49. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;

2.9.50. Criação e ativação de regras de acesso e perfis de acesso à rede;

2.9.51. Configuração de parâmetros de qualidade de serviço (QoS);

2.9.52. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;

2.9.53. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;

2.9.54. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;

2.9.55. Ativação e teste das ACLs nos equipamentos fornecidos;

2.9.56. Homologação

2.9.57. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.

2.9.58. Documentação em formato PDF contendo os itens a seguir:

2.9.59. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.

2.9.60. Arquivos de configuração dos ativos de rede;

2.9.61. Backup das configurações dos softwares utilizados;

2.9.62. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega;

2.10. Requisitos para instalação do cabeamento

- 2.10.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;
- 2.10.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;
- 2.10.3. Conectorização e crimpagem dos cabos em ambos os extremos;
- 2.10.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;
- 2.10.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;
- 2.10.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;
- 2.10.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;
- 2.10.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

2.11. Descrição do suporte continuado

- 2.11.1. A CONTRATADA deverá prestar assistência em horário comercial, das 07:30 às 16:30h na modalidade 8x5;
- 2.11.2. A CONTRATADA deverá providenciar a imediata reposição de equipamentos que estejam indisponíveis, seja por manutenção preventiva, seja por manutenção corretiva, avarias, acidentes ou paralisados por falhas provocadas por falta de suprimento, no prazo máximo de 24 (vinte e quatro) horas;

2.11.3. Da Manutenção Preventiva

A Contratada é a única e exclusiva responsável pela manutenção preventiva dos equipamentos objeto desta contratação; A manutenção deve obedecer às recomendações do fabricante de cada equipamento, porém, sem se limitar a elas e aos serviços abaixo descritos:

- 2.11.4. Providenciar revisão geral de todos os itens previstos de acordo com a recomendação do fabricante;
- 2.11.5. Verificar o estado geral de conservação dos equipamentos e providenciar substituição dos mesmos sempre que for necessário;
- 2.11.6. Efetuar as revisões periódicas, observando as recomendações do fabricante;
- 2.11.7. A Contratada deverá realizar as manutenções preventivas para garantir o pleno funcionamento dos equipamentos e a qualidade dos materiais produzidos.

2.11.8. Manutenção Corretiva

- 2.11.9. A manutenção corretiva deverá ocorrer sempre que a substituição do equipamento for necessária por quebra, assim como quando surgirem falhas;
- 2.11.10. A CONTRATADA deverá iniciar a manutenção corretiva em um prazo máximo de 4 (quatro) horas após a notificação por parte da CONTRATANTE, respeitando os horários definidos pela CONTRATANTE para essa tarefa;
- 2.11.11. A CONTRATADA deverá arcar com todos os custos decorrentes de avarias, exceto os decorrentes do mau uso do equipamento por parte do Contratante; Nesses casos, será de responsabilidade do Contratante arcar com os custos de reparo do equipamento;
- 2.11.12. A CONTRATADA deverá assumir integral e absoluta responsabilidade pelos equipamentos locados, desobrigando a CONTRATANTE de qualquer ônus, encargos, deveres e responsabilidade por defeitos, vícios aparentes ou ocultos, ou funcionamento insatisfatório dos aludidos bens e acidentes.

2.11.13. Serviço continuado

- 2.11.14. CONTRATADA deverá assumir a responsabilidade pelo gerenciamento da WLAN no que tange as seguintes ações:
- 2.11.15. Provisionamento e descoberta de dispositivos;
- 2.11.16. Prestar suporte técnico remoto e presencial;
- 2.11.17. Realizar atualizações de firmware e patches de segurança nos equipamentos;
- 2.11.18. Fazer a gestão de capacidade, espectro e canais da rede wireless;
- 2.11.19. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 2.11.20. Monitorar continuamente a saúde dos dispositivos
- 2.11.21. Monitorar perfil de usuário;
- 2.11.22. Monitorar Autenticação de usuários;
- 2.11.23. Proteção e implementação de WLAN usando os protocolos de segurança descritos no TR;
- 2.11.24. Entregar relatórios mensais com análise de disponibilidade, uso de canais, desempenho e incidentes;
- 2.11.25. Substituir equipamentos com defeito conforme cláusulas de SLA;
- 2.11.26. Corrigir falhas em conectores, cabos, patch panels e pontos RJ45 usados na solução;

2.12. ITEM - FIREWALL (SEDE)

- 2.12.1. Características da solução
 - 2.12.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
 - 2.12.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
 - 2.12.1.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
 - 2.12.1.4. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
 - 2.12.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução
 - 2.12.1.6. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço
 - 2.12.1.7. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.
 - 2.12.1.8. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.12.2. Requisitos técnicos dos equipamentos que compõe a solução

- 2.12.2.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.12.2.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;
- 2.12.2.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;
- 2.12.2.4. Deve Suportar, no mínimo, 65.000 (sessenta e cinco mil) Conexões de throughput VPN IPSec

- 2.12.2.4. Deve suportar, no mínimo, 0,5 (seis virgula cinco) Gbps de throughput VPN IPsec;
- 2.12.2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;
- 2.12.2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;
- 2.12.2.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;
- 2.12.2.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
- 2.12.2.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.
- 2.12.2.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;
- 2.12.2.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;
- 2.12.2.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;
- 2.12.2.13. Deve possuir porta console RJ-45;
- 2.12.2.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;
- 2.12.2.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
- 2.12.2.16. Deve possuir Fontes redundantes.
- 2.12.2.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.
- 2.12.2.18. Deve ser licenciado para uso pelo período de duração do contrato.
- 2.12.2.19. Deve possuir garantia para uso pelo período de duração do contrato.
- 2.12.3. Firewalls de próxima geração (NGFW).
- 2.12.3.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
- 2.12.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.12.3.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 2.12.3.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 2.12.3.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
- 2.12.3.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.
- 2.12.3.7. Funcionalidades de rede e firewall.**
- 2.12.3.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 2.12.3.7.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 2.12.3.7.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.12.3.7.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 2.12.3.7.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.12.3.7.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
- 2.12.3.7.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.12.3.7.8. Deverá suportar sFlow ou Netflow;
- 2.12.3.7.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 2.12.3.7.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 2.12.3.7.11. Deve suportar o protocolo padrão da indústria VXLAN;
- 2.12.3.7.12. Deve implementar o protocolo ECMP;
- 2.12.3.7.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 2.12.3.7.14. Enviar log para sistemas de monitoração externos;
- 2.12.3.7.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 2.12.3.7.16. Deve possuir mecanismos de proteção anti-spoofing;
- 2.12.3.7.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 2.12.3.7.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.12.3.7.19. Suportar OSPF graceful restart;
- 2.12.3.7.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.12.3.7.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 2.12.3.7.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 2.12.3.7.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 2.12.3.7.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 2.12.3.7.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 2.12.3.7.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 2.12.3.7.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 2.12.3.7.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 2.12.3.7.31. Deverá suportar controle por zonas de segurança;
- 2.12.3.7.32. Deverá suportar controles de políticas por porta e protocolo;
- 2.12.3.7.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 2.12.3.7.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 2.12.3.7.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 2.12.3.7.36. Controle, inspeção e descifração de SSL por política para tráfego de saída (Outbound).

2.12.3.7.36. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
2.12.3.7.37. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
2.12.3.7.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
2.12.3.7.39. Suporte a objetos e regras IPV6;
2.12.3.7.40. Suporte a objetos e regras multicast;
2.12.3.7.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

2.12.3.8. Funcionalidade de controle de aplicações.

2.12.3.8.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2.12.3.8.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
2.12.3.8.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
2.12.3.8.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
2.12.3.8.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
2.12.3.8.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
2.12.3.8.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
2.12.3.8.8. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
2.12.3.8.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
2.12.3.8.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
2.12.3.8.11. Atualizar a base de assinaturas de aplicações automaticamente;
2.12.3.8.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
2.12.3.8.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
2.12.3.8.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
2.12.3.8.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
2.12.3.8.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
2.12.3.8.17. Deve alertar o usuário quando uma aplicação for bloqueada;
2.12.3.8.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
2.12.3.8.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
2.12.3.8.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
2.12.3.8.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
2.12.3.8.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

2.12.3.9. Funcionalidade de prevenção de intrusão de ameaças.

2.12.3.9.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
2.12.3.9.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
2.12.3.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
2.12.3.9.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e "quarentenar" IP do atacante por um intervalo de tempo;
2.12.3.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
2.12.3.9.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
2.12.3.9.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
2.12.3.9.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
2.12.3.9.9. Deve permitir o bloqueio de vulnerabilidades;
2.12.3.9.10. Deve permitir o bloqueio de exploits conhecidos;
2.12.3.9.11. Deve incluir proteção contra-ataques de negação de serviços;
2.12.3.9.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
2.12.3.9.13. Detectar e bloquear a origem de portscans;
2.12.3.9.14. Bloquear ataques efetuados por worms conhecidos;
2.12.3.9.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
2.12.3.9.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
2.12.3.9.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

- 2.12.3.9.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.12.3.9.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.12.3.9.20. Identificar e bloquear comunicação com botnets;
- 2.12.3.9.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.12.3.9.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 2.12.3.9.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.12.3.9.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 2.12.3.9.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 2.12.3.9.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 2.12.3.9.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 2.12.3.9.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

2.12.3.10. Funcionalidade de filtro de conteúdo web e dns.

- 2.12.3.10.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.12.3.10.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 2.12.3.10.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 2.12.3.10.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 2.12.3.10.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.12.3.10.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 2.12.3.10.7. Possuir pelo menos 70 (setenta) categorias de URLs;
- 2.12.3.10.8. Deve possuir a função de exclusão de URLs do bloqueio;
- 2.12.3.10.9. Permitir a customização de página de bloqueio;
- 2.12.3.10.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 2.12.3.10.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 2.12.3.10.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 2.12.3.10.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

2.12.3.11. Funcionalidade de identificação de usuários.

- 2.12.3.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
- 2.12.3.11.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 2.12.3.11.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 2.12.3.11.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 2.12.3.11.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 2.12.3.11.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.12.3.11.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 2.12.3.11.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

2.12.3.12. Funcionalidade de filtro de dados .

- 2.12.3.12.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 2.12.3.12.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.12.3.13. Funcionalidade de geolocalização.

- 2.12.3.13.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 2.12.3.13.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.12.3.14. Funcionalidade de vpn.

- 2.12.3.14.1. Suportar VPN Site-to-Site e Cliente-To-Site;
- 2.12.3.14.2. Suportar IPSec VPN;
- 2.12.3.14.3. A VPN IPSEC deve suportar 3DES;
- 2.12.3.14.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 2.12.3.14.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

- 2.12.3.14.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.12.3.14.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.12.3.14.8. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 2.12.3.14.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.12.3.14.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPsec IPv6;
- 2.12.3.14.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.12.3.14.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 2.12.3.14.13. Atribuição de DNS nos clientes remotos de VPN;
- 2.12.3.14.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 2.12.3.14.15. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 2.12.3.14.16. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.12.3.14.17. Deverá manter uma conexão segura com o portal durante a sessão;
- 2.12.3.14.18. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

2.12.3.15. Funcionalidade de qos, traffic shaping e priorização de tráfego.

- 2.12.3.15.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- 2.12.3.15.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
- 2.12.3.15.3. Endereço de origem e Endereço de destino;
- 2.12.3.15.4. Usuário e grupo;
- 2.12.3.15.5. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 2.12.3.15.6. Por porta;
- 2.12.3.15.7. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 2.12.3.15.8. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
- 2.12.3.15.9. O QoS deve possibilitar a definição de fila de prioridade;
- 2.12.3.15.10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 2.12.3.15.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 2.12.3.15.12. Suportar modificação de valores DSCP para o Diffserv;
- 2.12.3.15.13. Suportar priorização de tráfego usando informação de ToS (Type of Service);
- 2.12.3.15.14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 2.12.3.15.15. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- 2.12.3.15.16. Deve possibilitar a definição de bandas distintas para download e upload;

2.12.3.16. Funcionalidade de balanceamento inteligente de links.

- 2.12.3.16.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 2.12.3.16.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
- 2.12.3.16.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 2.12.3.16.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 2.12.3.16.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 2.12.3.16.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 2.12.3.16.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
- 2.12.3.16.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 2.12.3.16.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 2.12.3.16.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
- 2.12.3.16.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 2.12.3.16.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 2.12.3.16.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 2.12.3.16.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 2.12.3.16.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 2.12.3.16.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 2.12.3.16.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

2.12.3.16.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

2.12.3.16.19. A solução deve possuir recurso para controlar e corrigir erros (FEC - Forward Error Correction) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

2.12.3.16.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

2.12.3.16.21. A solução deve suportar nativamente conectores com clouds públicas;

2.12.3.16.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

2.12.3.16.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

2.12.3.16.24. Deve implementar balanceamento de link por hash do IP de origem;

2.12.3.16.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

2.12.3.16.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

2.12.3.16.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

2.12.3.16.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

2.12.3.17. Funcionalidade de controlador de rede sem fio.

2.12.3.17.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

2.12.3.17.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

2.12.3.17.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

2.12.3.17.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

2.12.3.17.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

2.12.3.17.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

2.12.3.17.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

2.12.3.17.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de **túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

2.12.3.17.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPsec;

2.12.3.17.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.12.3.17.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.12.3.17.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

2.12.3.17.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

2.12.3.17.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.12.3.17.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

2.12.3.17.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

2.12.3.17.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

2.12.3.17.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como **Rogue APs**. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

2.12.3.17.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

2.12.3.17.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

2.12.3.17.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

2.12.3.17.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

2.12.3.17.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID

2.12.3.17.23. A solução deve permitir o agrupamento de pontos de acesso para que sejam distribuídas múltiplas subredes em um determinado sub, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

2.12.3.17.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

2.12.3.17.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

2.12.3.17.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

2.12.3.17.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.12.3.17.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.12.3.17.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.12.3.17.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

2.12.3.17.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

2.12.3.17.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

2.12.3.17.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.12.3.17.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

2.12.3.17.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

2.12.3.17.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

2.12.3.17.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;

2.12.3.17.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.12.3.17.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

2.12.3.17.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

2.12.3.17.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

2.12.3.17.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

2.12.3.17.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

2.12.3.17.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

2.12.3.17.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

2.12.3.17.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES)**;

2.12.3.17.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

2.12.3.17.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

2.12.3.17.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

2.12.3.17.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.12.3.17.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

2.12.3.17.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.12.3.17.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

2.12.3.17.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

2.12.3.17.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

2.12.3.17.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

2.12.3.17.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

2.12.3.17.58. A solução deve permitir a configuração do captive portal com endereço IPv6;

2.12.3.17.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

2.12.3.17.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

2.12.3.17.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

2.12.3.17.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

2.12.3.17.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

2.12.3.17.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

2.12.3.17.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será

disponibilizado;

2.12.3.17.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

2.12.3.17.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

2.12.3.17.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

2.12.3.17.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

2.12.3.17.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

2.12.3.17.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

2.12.3.17.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo **SNMP**;

2.12.3.17.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

2.12.3.17.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

2.12.3.17.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

2.12.3.17.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

2.12.3.17.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

2.12.3.17.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

2.12.3.17.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

2.12.3.17.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

2.12.3.17.81. A solução deve possuir ferramentas de diagnósticos e debug;

2.12.3.17.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

2.12.3.17.83. A solução deve suportar comunicação com elementos externos através de REST API;

2.12.3.17.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

2.12.3.18. Funcionalidade de controlador de rede cabeada.

2.12.3.18.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

2.12.3.18.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

2.12.3.18.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

2.12.3.18.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

2.12.3.18.5. Deve montar a topologia da rede de maneira automática;

2.12.3.18.6. Deve ser capaz de configurar os switches da rede;

2.12.3.18.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches

gerenciados;

2.12.3.18.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

2.12.3.18.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

2.12.3.18.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

2.12.3.18.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

2.12.3.18.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

2.12.3.18.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

2.12.3.18.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

2.12.3.18.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

2.12.3.18.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

2.12.3.18.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

2.12.3.18.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

2.12.3.18.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

2.12.3.18.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

2.12.3.18.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

2.12.3.18.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

2.12.3.18.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

2.12.3.18.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

2.13. Serviço de instalação firewall

2.13.1. Instalação Estrutura Física

2.13.1.1. Levantamento de toda estrutura física do ambiente;

2.13.1.2. Levantamento da estrutura Elétrica;

2.13.1.3. Verificação do espaço a ser instalado os equipamentos;

2.13.1.4. Abertura e conferência das caixas dos equipamentos;

2.13.1.5. Instalação do appliance físico;

2.13.1.6. Fixação do equipamento no RACK;

2.13.1.7. Conexão da fonte de alimentação elétrica em régua de tomada;

2.13.1.8. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;

2.13.1.9. Conexão das interfaces de rede com os switches;

2.13.2. Configuração do appliance físico:

2.13.2.1. Parametrização do Licenciamento;

- 2.13.2.2. Parametrização das interfaces de rede;
- 2.13.2.3. Atualização da última versão de Firmware;
- 2.13.2.4. Parametrização das regras de NAT;
- 2.13.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 2.13.2.6. Parametrização de Controle de Aplicação;
- 2.13.2.7. Parametrização de VPN (Virtual Private Network);
- 2.13.2.8. Parametrização IDS/IPS;
- 2.13.2.9. Parametrização DNS;
- 2.13.2.10. Parametrização de Gateway Antivírus;
- 2.13.2.11. Parametrização de Objetos de Endereço;
- 2.13.2.12. Parametrização de Grupo de Objetos;
- 2.13.2.13. Parametrização de Load Balancing;
- 2.13.2.14. Parametrização de SSO (Single Sign-on);
- 2.13.2.15. Parametrização de SNMP;
- 2.13.2.16. Parametrização de NTP;
- 2.13.2.17. Parametrização de PortGroups;
- 2.13.2.18. Parametrização de Zones;
- 2.13.2.19. Parametrização de Serviços;
- 2.13.2.20. Parametrização de Rotas;
- 2.13.2.21. Parametrização de DHCP

2.14. Serviços profissionais de suporte técnico na solução de firewall

- 2.14.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;
- 2.14.2. Efetuar toda rotina de backup das configurações semanalmente;
- 2.14.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

2.14.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

- 2.14.4.1. Atividades relativas à Solução de Segurança:
- 2.14.4.2. Criação das rotas para links.
- 2.14.4.3. Criação de NAT.
- 2.14.4.4. Liberação de portas.
- 2.14.4.5. Configuração do Filtro de Conteúdo.
- 2.14.4.6. Configuração do Controle de Aplicativos.
- 2.14.4.7. Configuração do Agente para autenticação LDAP.
- 2.14.4.8. Configuração para o Single Sign-On (SSO).
- 2.14.4.9. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 2.14.4.10. Configuração de VPN client to site.
- 2.14.4.11. Configuração de VPN site to site.
- 2.14.4.12. Criação de regras de Firewall.
- 2.14.4.13. Criação de regras de QoS.
- 2.14.4.14. Emitir relatório de segurança mensal por localidade.
- 2.14.4.15. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 2.14.4.16. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.
- 2.14.4.17. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

2.14.5. SLA dos serviços e atendimento

- 2.14.5.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 2.14.5.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 2.14.5.3. Gerar relatórios de acesso e desempenho da solução de firewall.
- 2.14.5.4. Deverá possuir sistema de abertura de chamados pela internet.
- 2.14.5.5. Monitorar latência e uptime dos links configurados.
- 2.14.5.6. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 2.14.5.7. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 2.14.5.8. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 2.14.5.9. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade

1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma

	continua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

2.15. Níveis de Severidade

2.15.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

2.15.2. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (quatro) horas úteis após o registro do chamado.

2.15.2.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

2.15.2.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.3. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.3.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser on-site e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

2.15.3.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.4. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.4.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência.

2.15.4.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.5. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.5.1. A CONTRATADA terá, no máximo, 8 (oito) dias corridos para solucionar o chamado, após o seu registro.

2.15.5.2. Não poderá haver limites no quantitativo de abertura de chamados.

2.16 Qualificação Técnica

2.16.1. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

2.16.2. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

2.16.3. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

2.16.4. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas;

2.16.5. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan, sendo que os trechos da documentação que comprovem os respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização.

3. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

3.1. Definição do objeto

3.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (Físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, firewall

(SonicWall), nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

3.1.2. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21 da Lei nº 14.133, de 2021.

3.1.3. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar.

3.1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

3.1.5. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

3.1.6. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

3.2. Características da solução

3.2.1. A execução do objeto seguirá a seguinte dinâmica:

3.2.2. Início da execução do objeto: 05 (cinco) dias úteis da emissão da ordem de serviço;

3.2.3. Descrição detalhada:

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

3.2.4. Contratada deve prestar os serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente.

3.2.5. A empresa deverá estar pronta para gerir toda a estrutura hiperconvergente, que conta atualmente com dois clusters gerenciados de forma separada (com armazenamento baseado em Software-defined storage -SDS), uma infraestrutura com base em acessos VDI, máquinas virtuais. A empresa contratada deve estar pronta para lidar com seus backups, restores, e qualquer problema, falha, atualização, instalação ou análise oriunda desta relação de ferramentas integradas.

3.3. Requisitos técnicos

3.3.1. Monitoramento e suporte técnico

3.3.2. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;

3.3.3. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:

3.3.4. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);

3.3.5. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;

3.3.6. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;

3.3.7. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

3.3.8. Manutenção, gestão de ativos e rede

3.3.9. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados no item 6.1.1, sem custo adicional;

3.3.10. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;

3.3.11. Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.

3.3.12. Executar a gestão técnica da infraestrutura de rede, abrangendo:

3.3.13. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;

3.3.14. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;

3.3.15. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;

3.3.16. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.

3.3.17. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

3.3.18. Serviços gerenciados

3.3.19. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;

3.3.20. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;

3.3.21. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;

3.3.22. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

3.3.23. Controle, inventário e chamados

3.3.24. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;

3.3.25. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

3.3.26. Logística e apoio à contratação

3.3.27. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;

3.3.28. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:

3.3.29. Elaboração de especificações técnicas;

3.3.30. Análise de propostas técnicas;

3.3.31. Apoio em processos licitatórios;

3.3.32. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

3.3.33. Atendimento presencial

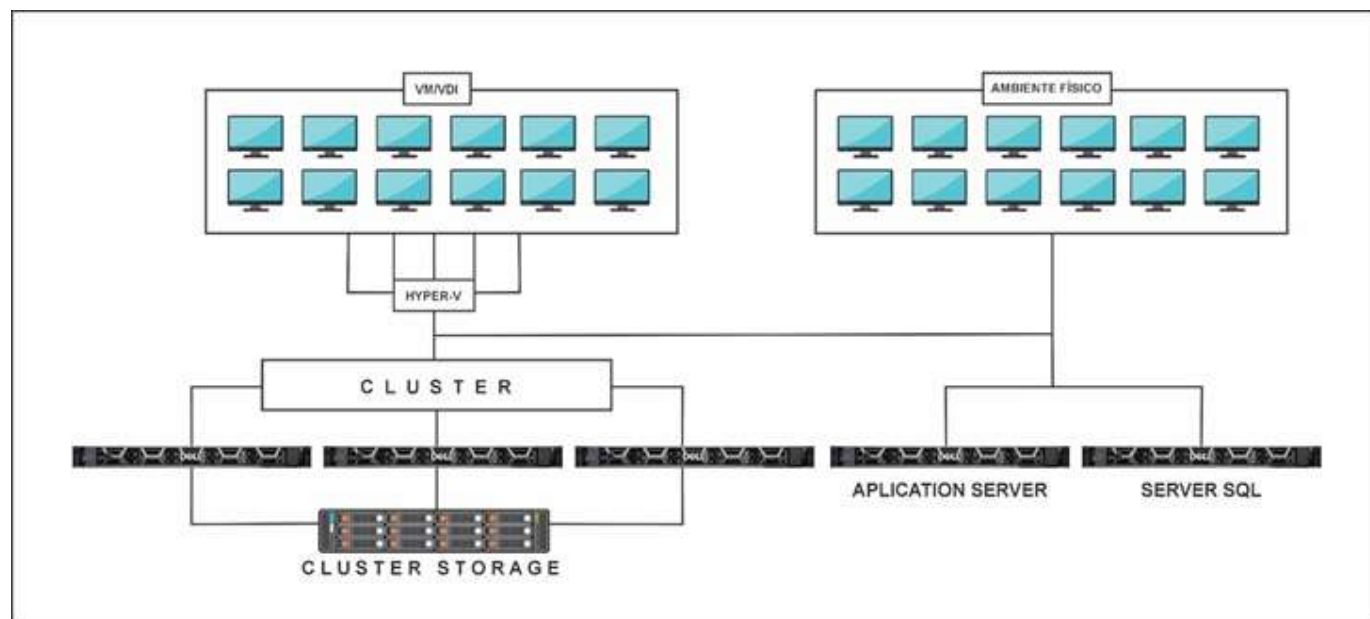
3.3.34. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 8 (oito) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

3.3.35. Parque de informática do CRCES:

TIPO	DESCRIÇÃO	QUANTIDADE
Equipamento de segurança	Firewall a ser contratado neste termo de referência	01
Pontos de acesso	Pontos de acesso a serem contratados neste termo de referência	A depender da solução contratada
Virtualizador	Hyper-V	05
Servidor Windows 2022 Server	Dell PowerEdge R640	02
Servidor Windows 2022 Server	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01
Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01

Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados - VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01

3.3.36. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



3.3.36. Manutenção Preventiva e Corretiva

3.3.36.1. Manutenção Preventiva

3.3.36.1.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

3.3.36.1.2. Tais atividades incluem, mas não se limitam a:

3.3.36.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

- 3.3.36.1.2.2. Limpeza técnica interna e externa;
- 3.3.36.1.2.3. Aferição e calibração de dispositivos, quando aplicável;
- 3.3.36.1.2.4. Atualização de firmwares, BIOS e softwares;
- 3.3.36.1.2.5. Verificação e otimização de configurações;
- 3.3.36.1.2.6. Avaliação do desempenho geral e análise de logs;
- 3.3.36.1.2.7. Testes de funcionalidade e conectividade.
- 3.3.36.1.3. Os equipamentos e ativos de tecnologia que deverão ser contemplados no plano de manutenção preventiva incluem:
 - 3.3.36.1.3.1. Servidores físicos;
 - 3.3.36.1.3.2. Servidores virtuais;
 - 3.3.36.1.3.3. Infraestrutura de rede (switches, cabeamento, racks, patch panels, etc.);
 - 3.3.36.1.3.4. Ativos de rede (roteadores, access points, controladoras, etc.);
 - 3.3.36.1.3.5. Estações de trabalho tipo desktop;
 - 3.3.36.1.3.6. Nobreaks e sistemas de energia ininterrupta;
 - 3.3.36.1.3.7. Terminais de desktop virtualizado (Thin Clients);
 - 3.3.36.1.3.8. Firewalls e appliances de segurança;
 - 3.3.36.1.3.9. Notebooks;
 - 3.3.36.1.3.10. Scanners (digitalizadores) de mesa e portáteis;
 - 3.3.36.1.3.11. Projetores multimídia;
 - 3.3.36.1.3.12. Monitores LCD/LED;
 - 3.3.36.1.3.13. Telefones IP e demais dispositivos de comunicação.
- 3.3.36.1.4. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.
- 3.3.36.1.5. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.
- 3.3.36.1.6. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.
- 3.3.36.1.7. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que solicitado.
- 3.3.36.2. Manutenção Corretiva
 - 3.3.36.2.1. Em caso de problema técnico, a contratada deverá providenciar laudo técnico e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.
 - 3.3.36.2.2. A CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.
 - 3.3.36.2.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.
 - 3.3.36.2.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.
 - 3.3.36.2.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.
 - 3.3.36.2.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 (cinco) dias úteis após o recebimento dos novos equipamentos/peças.
 - 3.3.36.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.
 - 3.3.36.2.8. Durante a execução do serviço externo, a empresa contratada deverá:
 - 3.3.36.2.8.1. Se responsabilizar pelo transporte dos equipamentos que serão retirados;
 - 3.3.36.2.8.2. Providenciar termo de responsabilidade de retirada;
 - 3.3.36.2.8.3. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.
 - 3.3.36.2.9. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;
 - 3.3.36.2.10. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;
 - 3.3.36.2.11. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;
 - 3.3.36.2.12. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;
 - 3.3.36.2.13. O recebimento definitivo não transfere a responsabilidade futura perante a qualidade do produto entregue.

- 3.3.36.2.13. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto a qualidade do produto entregue;
- 3.3.36.2.14. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.
- 3.3.37. SLA dos Serviços e Atendimento**
- 3.3.37.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 3.3.37.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 3.3.37.3. O ambiente de TI do CRCES deverá ser continuamente monitorado por ferramentas especializadas, com alertas automáticos e registro de falhas, a fim de garantir o funcionamento adequado e a disponibilidade dos recursos.
- 3.3.37.4. Deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos.
- 3.3.37.5. Deverá possuir sistema de abertura de chamados pela internet.
- 3.3.37.6. Monitorar latência e uptime dos links configurados.
- 3.3.37.7. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 3.3.37.7.1. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela (a ser fornecida ou referenciada no documento original).
- 3.3.37.7.2. Os níveis de atendimento técnico (N1, N2 e N3) deverão seguir o escopo descrito no item 3.3, com suporte remoto ilimitado e visitas técnicas presenciais duas vezes por semana (conforme cláusula 3.3.34).
- 3.3.37.7.3. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 3.3.37.8. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela (a ser fornecida ou referenciada no documento original).

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética (“cosméticos”), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

3.3.38 Níveis de Severidade

- **3.3.38.1.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.
- **3.3.38.2.** Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime **8x5 (on-site ou remota)**, com atendimento no local em até **4 (horas) horas úteis** após o registro do chamado.
 - **3.3.38.2.1.** Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a **8 (oito) horas úteis**, após o registro do chamado.
 - **3.3.38.2.2.** Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar **4 (quatro) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.3.** Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime **8x5 (remota ou on-site)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.3.1.** Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após **12 (doze) horas úteis**, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao **próximo dia útil**, após o registro do chamado.
 - **3.3.38.3.2.** Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.

- **3.3.38.4.** Para os chamados classificados como severidade 3 (tres), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.4.1.** A CONTRATADA terá, no máximo, **24 (Vinte e quatro) horas úteis**, após registro do chamado, para implantar uma solução definitiva ou de contingência.
 - **3.3.38.4.2.** Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias corridos** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.5.** Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.5.1.** A CONTRATADA terá, no máximo, **8 dias corridos** para solucionar o chamado, após o seu registro.
 - **3.3.38.5.2.** Não poderá haver limites no quantitativo de abertura de chamados.

3.3.39 Qualificação Técnica

- **3.3.39.1.** A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se inviável:
- **3.3.39.2.** Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- **3.3.39.3.** Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.
- **3.3.39.4.** Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.
- **3.3.39.5.** Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.
- **3.3.39.6.** Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.
- **3.3.39.7.** Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.
- **3.3.39.8.** Certificação ITIL v3 ou superior;
- **3.3.39.9.** Certificação MCSA Windows Server 2012 ou superior;
- **3.3.39.10.** A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:
 - **3.3.39.10.1.** Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;
 - **3.3.39.10.2.** Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;
 - **3.3.39.10.3.** Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

4. BACKUP CORPORATIVO

4.1. Software de Backup

- **4.1.1.** Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- **4.1.2.** Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.
- **4.1.3.** Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- **4.1.4.** Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.
- **4.1.5.** Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.
- **4.1.6.** Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- **4.1.7.** Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.
- **4.1.8.** Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.
- **4.1.9.** Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.
- **4.1.10.** Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.
- **4.1.11.** Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.
- **4.1.12.** Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.

- 4.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações:** O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.
- 4.1.14. Backup Incremental e Diferencial:** Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.
- 4.1.15. Cópias de Backup Imutáveis:** Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.
- 4.1.16. Retenção Personalizável:** O software deve oferecer flexibilidade na configuração de políticas de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.
- 4.1.17. Arquivamento Inteligente:** Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.
- 4.1.18. Monitoramento e Alertas:** O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.
- 4.1.19. Dashboard Intuitivo:** Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.
- 4.1.20. Otimização de Recursos (IOPS e Throughput):** O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.
- 4.1.21. Restauração Granular:** Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.
- 4.1.22. Recuperação Bare-Metal:** Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.
- 4.1.23. Testes de Restauração Automática:** Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.
- 4.1.24. Integração Nativa com Provedores de Nuvem:** Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.
- 4.1.25. Economia de Largura de Banda:** Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.
- 4.1.26. Perfis de Acesso Personalizáveis:** O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.
- 4.1.27. Controle de Acessos Granular:** Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.
- 4.1.28. Suporte a LGPD e Outras Normas:** O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.
- 4.1.29. Auditorias e Relatórios:** Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.
- 4.1.30. Automatização de trabalhos de Backup:** Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.
- 4.1.31. Integração com Ferramentas de Orquestração:** Suporte para integração com ferramentas de orquestração e automação (ex: scripts PowerShell, APIs).
- 4.1.32. Cobertura Completa:** O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.
- 4.1.33. Recuperação Granular:** Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.
- 4.1.34. Agendamento e Automação:** A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

4.2. Appliance de Backup Local

- 4.2.1.** A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.
- 4.2.2.** Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.
- 4.2.3.** Será responsável por configurar o sistema de armazenamento local do equipamento, devendo:
- 4.2.3.1.** Criar e configurar o arranjo de discos em RAID 5;
- 4.2.3.2.** Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);
- 4.2.3.3.** Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas
- 4.2.4.** Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.
- 4.2.5.** Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:
- 4.2.5.1.** Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;
- 4.2.5.2.** Gerar e manter registros e relatórios de status dos backups locais e remotos;
- 4.2.5.3.** Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC ES.

4.2.5.5. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

4.2.6. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:

4.2.6.1. Acompanhamento da integridade dos discos e volumes lógicos;

4.2.6.2. Monitoramento do uso de espaço em disco e alertas proativos;

4.2.6.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

4.2.7. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:

4.2.7.1. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;

4.2.7.2. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).

4.2.8. deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:

4.2.8.1. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;

4.2.8.2. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;

4.2.8.3. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;

4.2.8.4. Ajustar as políticas de backup e monitoramento para o novo ambiente.

4.2.9. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

4.3. Armazenamento de backup em nuvem

4.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.

4.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.

4.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.

4.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.

4.3.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.

4.3.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.

4.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.

4.3.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).

4.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.

4.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.

4.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.

4.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.

4.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.

4.3.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.

4.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.

4.3.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.

4.3.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.

4.3.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).

4.3.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.

4.3.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e possíveis falhas.

4.3.23. Ferramentas de monitoramento nativas devem estar integradas.

4.3.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

4.4. SLA dos serviços e atendimento

- 4.4.1.** Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 4.4.2.** Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 4.4.3.** deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime e falhas críticas.
- 4.4.4.** Deverá possuir sistema de abertura de chamados pela internet.
- 4.4.5.** A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 4.4.6.** O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 4.4.7.** Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 4.4.8.** Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela , a seguir:

Níveis de Severidade	
1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.

3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup..
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

4.4.9. Níveis de Severidade

4.4.10. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

4.4.11. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

4.4.11.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

4.4.11.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

4.4.12. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

4.4.12.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

4.4.12.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

4.4.13. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

4.4.13.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

4.4.13.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

4.4.14. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

4.4.14.1. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

4.4.14.2. Não poderá haver limites no quantitativo de abertura de chamados.

4.3.3.17. Certificações

Será necessário solicitar algumas certificações, com isso o CRCES está garantindo que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade, alinhado com as melhores práticas do mercado e com as recomendações de segurança de órgãos como o NIST e o CIS.

Abaixo, vamos citar cada uma delas, ampliando as justificativas:

a) Certificação Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 (no mínimo)

Domínio do Sistema Operacional: A certificação MCSA garante que o profissional possui um conhecimento profundo do Windows Server 2012,

que é a base do nosso ambiente corporativo hiperconvergente. Isso inclui domínio em instalação, configuração, administração e troubleshooting do sistema operacional, além de serviços como Active Directory, DNS, DHCP e outros.

Integração com Outros Serviços: O Windows Server é integrado a outros serviços da Microsoft, como Exchange, SharePoint e SQL Server. Um profissional com a certificação MCSA terá mais facilidade em integrar e gerenciar esses serviços em um ambiente unificado.

Padrão de Qualidade e Alinhamento com Boas Práticas: A certificação MCSA é reconhecida mundialmente como um padrão de qualidade para profissionais de infraestrutura. Ela demonstra que o profissional possui as habilidades necessárias para lidar com as complexidades de um ambiente como o nosso, que possui dois clusters e funciona no modelo de hiperconvergência, além de estar alinhado com as melhores práticas do mercado.

b) Certificação para Instalação e Configuração de Switches DELL ou similar

Infraestrutura de Rede e Otimização: Switches são equipamentos essenciais para a interconexão de dispositivos em uma rede. A certificação garante que o profissional possui conhecimento sobre os princípios de funcionamento de switches, além de saber como configurá-los para atender às necessidades específicas da rede do CRCES, que utiliza switches complexos de alta tecnologia (tanto o core quanto o de agregação da hiperconvergência). Isso permite otimizar o desempenho da rede, reduzindo a latência e aumentando a disponibilidade.

Escalabilidade e Flexibilidade: À medida que a rede cresce, é necessário adicionar novos switches. Um profissional certificado terá as habilidades necessárias para integrar novos switches à rede existente, garantindo a escalabilidade da infraestrutura e a flexibilidade para atender às futuras demandas do CRCES.

Alinhamento com as Melhores Práticas: A certificação garante que o profissional está familiarizado com as melhores práticas de configuração e gerenciamento de redes, o que contribui para a estabilidade e a segurança da infraestrutura.

As certificações solicitadas demonstram que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade para o CRCES. Elas garantem que os profissionais terão a capacidade de:

Gerenciar e manter a infraestrutura de TI de forma eficiente, segura e alinhada com as melhores práticas do mercado.

Resolver problemas de forma rápida e eficaz, minimizando o tempo de inatividade do sistema.

Implementar novas tecnologias de forma adequada e segura.

Acompanhar as melhores práticas do mercado e as recomendações de segurança de órgãos como o NIST e o CIS.

4.3.3.17.1. Justificativa

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada para gerar todos esses serviços de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a) Assegurar a contratação da empresa mais qualificada e experiente para o serviço.**
- b) Definir claramente as expectativas e responsabilidades de ambas as partes.**
- c) Permitir a avaliação objetiva das propostas e a escolha da melhor solução.**
- d) Facilitar o acompanhamento e a fiscalização do contrato.**
- e) Mitigar riscos e garantir o sucesso da contratação.**
- f) Atender aos princípios da Lei 14.133 e da Administração Pública.**

Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:

- a) Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.**
- b) Aumento de custos com retrabalho, correções e possíveis perdas.**
- c) Dificuldades na comunicação e na resolução de conflitos.**
- d) Dificuldades na fiscalização do contrato e na cobrança de resultados.**
- e) Riscos de inadimplência e de litígios.**

A contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.

4.3.3.18. Softwares que deverão ser disponibilizados

As ferramentas listadas abaixo (monitoramento e de abertura de chamados) deverão ser disponibilizadas e totalmente configuradas pela CONTRATADA sem custo adicional para o CRCES, e deverão apresentar as seguintes especificações (mínimas):

4.3.3.18.1. Ferramenta de monitoramento.

Monitoramento de Rede: Roteadores, switches, impressoras, etc., utilizando protocolos como SNMP (v1/v2c/v3), ICMP (ping) e verificações de portas TCP/UDP.

Monitoramento de Servidores: Desempenho de CPU, uso de memória, espaço em disco, tráfego de rede, processos, serviços e logs.

Monitoramento de Aplicações e Serviços: Bancos de dados (MySQL, PostgreSQL, Oracle, etc.), servidores web (Apache, Nginx, IIS), Java applications (JMX), serviços específicos e outros.

Monitoramento de Virtualização: Serviços em nuvem, contêineres, máquinas virtuais.

Monitoramento Web (Web Scenarios): Simula a navegação de usuários em aplicações web, verificando a disponibilidade, o tempo de resposta e o conteúdo das páginas.

Monitoramento de Dispositivos IoT e Sensores: Coleta dados de uma variedade de sensores e dispositivos IoT.

Monitoramento de Logs e Eventos: Analisa arquivos de log em busca de padrões, erros, avisos ou atividades suspeitas.

Extensibilidade: Permitir a coleta de dados qualquer fonte através de scripts externos personalizados, APIs e extensões.

Limiares Flexíveis: Definição de condições personalizadas para identificar problemas (triggers).

Previsão de Tendências e Machine Learning: Funções preditivas que permitem prever quando um limiar será atingido, possibilitando ações proativas antes que um problema ocorra.

Níveis de Severidade: Classificação dos problemas por níveis de severidade (informação, aviso, médio, alto, desastre), facilitando a priorização.

Análise de Causa Raiz: Ajuda a identificar a causa subjacente dos problemas.

Canais de Notificação Diversos: Envio de alertas por e-mail, SMS, aplicativos de mensagens (Telegram, Slack, etc.), webhooks e scripts personalizados.

Escalonamento de Alertas: Configuração de fluxos de escalonamento para garantir que os alertas cheguem aos destinatários corretos em diferentes etapas.

Ações Automáticas (Auto-remediação): Possibilidade de executar comandos remotos automaticamente em resposta a um problema (ex: reiniciar um serviço, executar um script de correção).

Notificações Customizáveis: Mensagens de alerta personalizadas com informações relevantes sobre o problema.

Dashboards Personalizáveis: Criação de painéis de controle interativos com widgets para exibir métricas em tempo real, status de hosts, problemas, mapas de rede, gráficos e muito mais.

Gráficos Flexíveis: Geração de gráficos detalhados para visualizar dados históricos e tendências, com opções de personalização de tempo e exibição.

Mapas de Rede (Network Maps): Criação de representações visuais da infraestrutura, mostrando o status dos dispositivos e as interconexões.

Relatórios: Geração de relatórios de disponibilidade, desempenho e outros dados relevantes.

Visão de Negócio (SLA/KPI): Possibilidade de monitorar o desempenho dos serviços de TI em relação aos Acordos de Nível de Serviço (SLAs) e Indicadores Chave de Desempenho (KPIs).

Descoberta Automática de Rede (Network Discovery): Detecta automaticamente novos dispositivos na rede, facilitando a configuração inicial.

Auto-registro de Agentes (Agent Autoregistration): Permite que os agentes Zabbix se registrem automaticamente no servidor Zabbix, simplificando a implantação em grande escala.

Descoberta de Baixo Nível (Low-Level Discovery - LLD): Descobre automaticamente componentes de um host (ex: interfaces de rede, sistemas de arquivos, CPUs, partições de disco) e cria itens de monitoramento, triggers e gráficos para eles.

Modelos (Templates): Reutilização de configurações de monitoramento para diferentes tipos de hosts, agilizando a implantação e padronizando o monitoramento.

Sistema de Permissões: Controle granular de acesso baseado em funções e grupos de usuários.

Autenticação: Suporte a diferentes métodos de autenticação (interna, LDAP, SAML).

criptografia: Criptografia de todo o tráfego de monitoramento para garantir a segurança dos dados.

Alta Disponibilidade: Monitoramento contínuo.

4.3.3.18.2. Ferramenta de abertura e gestão de chamados de T.I

Abertura de chamados por e-mail: Integração com e-mail para que os chamados sejam criados automaticamente a partir de mensagens enviadas para um endereço específico.

Categorização e Priorização Automática: Possibilidade de pré-definir categorias (ex: "Problema de Software", "Solicitação de Hardware", "Acesso"), subcategorias e níveis de prioridade (ex: "Baixa", "Média", "Alta", "Crítica") com base no tipo de solicitação ou no usuário.

Anexos: Capacidade de anexar arquivos (screenshots, logs, documentos) para fornecer mais contexto ao chamado.

Atribuição Automática e Manual: Atribuição de chamados a agentes ou equipes com base em regras predefinidas (categoria, prioridade, departamento do usuário) ou atribuição manual pelos gerentes.

Filas de Atendimento: Organização dos chamados em filas específicas para cada equipe ou tipo de serviço.

Fluxos de Trabalho (Workflows): Definição de etapas e ações automatizadas para o ciclo de vida de um chamado (ex: Aberto -> Em Andamento -> Aguardando Usuário -> Resolvido -> Fechado).

Notificações Automáticas: Envio de e-mails ou notificações push para o usuário e para os agentes sobre o status do chamado, novas mensagens, resolução, etc.

Colaboração em Equipe: Permite que múltiplos agentes trabalhem em um mesmo chamado, com compartilhamento de informações e anotações.

Macros/Respostas Predefinidas: Modelos de respostas para perguntas frequentes, agilizando o atendimento.

Artigos e FAQs: Repositório central de artigos de solução de problemas, FAQs (perguntas frequentes), guias e procedimentos.

Busca Inteligente: Ferramenta de busca robusta que permite aos usuários e agentes encontrar informações relevantes rapidamente.

Sugestão de Soluções: Apresentar artigos da base de conhecimento aos usuários enquanto eles digitam seu problema no portal self-service, incentivando a auto-resolução.

Dashboards e Métricas: Visualização em tempo real de KPIs (Key Performance Indicators) como número de chamados abertos, chamados resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

Relatórios Customizáveis: Geração de relatórios sobre desempenho da equipe, tipos de chamados mais comuns, cumprimento de SLAs, tendências, etc.

Integração com a ferramenta de Monitoramento: Integração com a ferramenta de monitoramento proposto pela CONTRATADA, para que alertas de monitoramento possam gerar chamados automaticamente.

Controle de Acesso Baseado em Funções: Definição de permissões diferentes para usuários, agentes e administradores.

Acessibilidade: Interface amigável e acessível em diferentes dispositivos (desktop, mobile).

SLA (Service Level Agreement) Management:

Definição de SLAs para diferentes tipos de chamados, especificando tempo de resposta e tempo de resolução esperados.

Monitoramento automático do cumprimento dos SLAs, com alertas e escalonamentos caso os prazos estejam sendo excedidos.

Escalonamento automático para gerentes ou equipes superiores quando os SLAs estão em risco.

Histórico Completo do Chamado: Registro detalhado de todas as interações, atualizações, comentários e mudanças de status em um chamado.

Pesquisa Avançada: Facilidade para buscar chamados por ID, usuário, categoria, palavras-chave, etc.

4.3.3.19. Serviços externos que deverão ser acompanhados pela contratada

A CONTRATADA será um ponto focal e estratégico para o CRCES, atuando como o principal **elo de coordenação e intermediação** entre nossa instituição e as demais prestadoras de serviços de TI. Dada a complexidade e a interdependência de nossas operações tecnológicas, a **intervenção e o acompanhamento proativo** da CONTRATADA serão cruciais para garantir a fluidez e a eficácia de todas as interações e projetos. Atualmente, gerenciamos diversos contratos com terceiros, e essa carteira de fornecedores poderá se expandir conforme nossas necessidades evoluírem. Abaixo vamos listar alguns dos contratos:

- Serviço de fornecimento de software de gestão integrada (SpiderWare);
- Serviço de hospedagem do website e webservice do CRCES;
- Serviço de fornecimento de link de internet;
- Serviço de fornecimento de e-mail corporativo;
- Serviço de fornecimento de link SIP Trunk;
- Serviço de fornecimento de validador de assinaturas digitais;
- Serviço de fornecimento de atendente virtual por whatsapp;
- Serviço de outsourcing de impressão;
- Serviço de fornecimento de ePABX;

5. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE DÃO SUPORTE;

5.1 A estimativa de quantidade foi baseada na estrutura de tecnologia atual do CRCES, conforme descrito ao longo deste documento.

6. LEVANTAMENTO DE MERCADO, ANÁLISE DAS ALTERNATIVAS POSSÍVEIS E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO T I SOLUÇÃO A CONTRATAR;

6.1 O levantamento de mercado para contratação de empresa que preste serviço de gerenciamento de T.I e um processo que requer atenção, cuidado e critério, pois envolve a confiança e a parceria entre o contratante e o contratado.

6.2 Atualmente, o CRCES enfrenta um cenário desafiador na gestão de T.I, com apenas um funcionário dedicado a essa área. Esta escassez representa um risco significativo para a continuidade dos serviços e para a qualidade do atendimento oferecido aos usuários.

6.3 Ademais, o CRCES se depara com desafios crescentes, como a necessidade premente de adaptação às normas de governança, a demanda por inovação e modernização tecnológica, bem como a crescente complexidade dos processos e projetos de T.I.

6.4 Em um ambiente em constante evolução tecnológica, é essencial que o CRCES esteja alinhado com as mais recentes tendências e práticas em T.I. A falta de recursos e expertise interna dificulta a implementação de soluções inovadoras que possam impulsionar a eficiência e a eficácia das operações.

6.5 O serviço de gerenciamento de T.I são considerados serviços comuns, pois se enquadram na definição de atividades que podem ser prestadas por qualquer pessoa jurídica, sem exigência de qualificação específica ou exclusividade.

6.6 Uma vez que há diversas empresas que oferecem este serviço, optamos por consultar empresas que já têm experiência com a infraestrutura tecnológica do CRCES, o que nos permite obter uma pesquisa mais adequada à realidade e à necessidade do suporte e serviço que solicitamos no processo, com isso, alcançamos a estimativa descrita abaixo:

	VALOR ITEM I
Mensal	R\$40.000,00
Anual	R\$480.000,00

6.7 Analisando os orçamentos apresentados, o valor mensal para esta contratação ficou estimado em R\$ 40.000,00 (quarenta mil reais), sendo que o valor total para os 12 (doze) meses resulta no valor de R\$480.000,00 (quatrocentos e oitenta mil reais) para os serviços gerenciados em Tecnologia da Informação.

CC-0/2025 - Comissão Permanente de Contabilidade da Prefeitura Santa Helena - 4478-0/2025 - Termo de responsabilidade de entrega de prestação de serviços

6.9 Além disso, o Conselho Regional de Contabilidade do Espírito Santo, como órgão público, tem a responsabilidade de zelar pelo uso eficiente dos recursos financeiros. Portanto, a busca pelo menor preço em processos de contratação é uma prática comum para garantir a economicidade e maximizar o retorno sobre o investimento público.

6.10 Outro aspecto relevante é a transparência e a simplificação do processo de licitação proporcionadas pelo critério de "menor preço". Por ser um critério objetivo de verificação, ele facilita a análise das propostas pelos licitantes e pelos responsáveis pela fiscalização, promovendo assim a lisura e a competitividade do certame.

6.10 Por fim, considerando que os **Serviços gerenciados em Tecnologia da Informação** são essenciais para garantir a saúde e a segurança dos ocupantes das instalações do Conselho Regional de Contabilidade, a escolha do critério de "menor preço" permite contar com uma infraestrutura de tecnologia da informação (T.I) eficiente, segura e atualizada, que garanta o bom funcionamento dos sistemas internos e externos, a comunicação com os diversos públicos e a proteção dos dados sensíveis.

6.11 Dessa forma, o uso do critério de "menor preço" no processo de licitação para a contratação de serviços **Tecnologia da Informação** completa é uma escolha justificada e alinhada aos princípios da administração pública, visando garantir a eficiência, a transparência e o melhor aproveitamento dos recursos disponíveis.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Conforme documentos acostados aos autos, o valor estimado da contratação mensal é de R\$40.000,00 (quarenta mil reais) perfazendo o valor total de R\$480.000,00 (quatrocentos e oitenta mil reais).

Para fins de estimativa da presente contratação, procedeu-se à pesquisa direta com fornecedores, por meio de solicitação de proposta de preço por e-mail, cujo valor médio é apresentado acima.

A pesquisa está em conformidade com o art. 6º da Instrução Normativa SEGES/ME n.º 65/2021, realizamos a média dos orçamentos.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, INCLUSIVE DAS EXIGÊNCIAS RELACIONADAS À MANUTENÇÃO E À ASSISTÊNCIA TÉCNICA, QUANDO FOR O CASO;

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

Na descrição da solução, já estão incluídos todos os procedimentos, equipamentos, instalação e manutenções corretivas para a perfeita execução dos serviços.

9. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO;

A não viabilidade de parcelamento da solução se fundamenta na natureza integrada do objeto, que demanda uma abordagem unificada para garantir eficiência e consistência. Optar por consolidar os serviços em um único item considerou a coesão dos elementos a serem licitados e a sequência lógica de sua execução.

Adicionalmente, a fragmentação deste processo acarretaria à Administração um risco significativo, pois diferentes empresas, embora possam operar no mesmo setor, apresentam disparidades estruturais, logísticas e econômico-financeiras. Tal divisão resultaria em capacidades discrepantes de prestação de serviço, comprometendo a supervisão e expondo a execução dos contratos a possíveis desvios dos padrões estabelecidos.

Portanto, a decisão de não parcelar a contratação busca assegurar a coerência e a qualidade na entrega dos serviços, minimizando potenciais incongruências e garantindo a conformidade na execução do objeto.

10. RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS;

Pretende-se com a presente contratação, os resultados abaixo descritos:

- Aumentar a eficiência e a segurança dos sistemas de informação do CRCES, reduzindo os riscos de falhas, perdas ou vazamentos de dados.
- Garantir a continuidade das atividades do CRCES em caso de eventuais problemas técnicos, desastres naturais ou ataques cibernéticos, por meio de um plano de recuperação de desastres baseado em backup em nuvem.
- Otimizar os custos e os recursos do CRCES, evitando gastos desnecessários com infraestrutura, manutenção e atualização de equipamentos e softwares.
- Melhorar o atendimento e a satisfação dos profissionais da contabilidade e da sociedade em geral, oferecendo serviços de qualidade, rapidez e confiabilidade.

11. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Para a execução do objeto deste estudo, não há necessidade de nenhuma adequação do ambiente do órgão.

12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES;

Para o objeto deste estudo, não são necessárias contratações correlatas ou interdependentes.

13. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, QUANDO APLICÁVEL;

Não se aplica a esta contratação.

14. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA.

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada em gerenciamento de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a. Assegurar a contratação da empresa mais qualificada e experiente para o serviço.
- b. Definir claramente as expectativas e responsabilidades de ambas as partes.
- c. Permitir a avaliação objetiva das propostas e a escolha da melhor solução.
- d. Facilitar o acompanhamento e a fiscalização do contrato.
- e. Mitigar riscos e garantir o sucesso da contratação.
- f. Atender aos princípios da Lei 14.133 e da Administração Pública.
- g. Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:
 - h. Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.
 - i. Aumento de custos com retrabalho, correções e possíveis perdas.
 - j. Dificuldades na comunicação e na resolução de conflitos.
 - k. Dificuldades na fiscalização do contrato e na cobrança de resultados.
 - l. Riscos de inadimplência e de litígios.
- m. Em suma, a contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.
- n. Investir em um Termo de Referência bem elaborado é um investimento na segurança, confiabilidade e no sucesso da gestão da TI do CRCES.
- o. Além disso, essa medida promove transparência e integridade, uma vez que impede o envolvimento de terceiras partes que possam diluir a responsabilidade direta da contratada. A restrição à exploração industrial visa, ainda, assegurar que o objeto seja destinado exclusivamente ao cumprimento das finalidades públicas, sem desvios para utilização comercial ou industrial que contrariem o interesse público.
- p. Para comprovação de capacidade, deve exigir-se que os licitantes apresentem atestados técnicos que demonstrem a execução dos serviços com infraestrutura própria e sem uso de exploração industrial, atendendo assim ao critério de "estrutura própria" e garantindo os altos padrões esperados.

Com base nas informações estabelecidas neste documento, nas justificativas apresentadas no Documento de Formalização da Demanda – DFD, a Equipe de Planejamento DECLARA a viabilidade da contratação de empresa especializada, Serviços de TI inclui a gestão de redes, ativos de rede, servidores, estações de trabalho, nobreaks e monitores. A empresa será responsável por suporte técnico remoto e presencial, manutenção preventiva e corretiva, e monitoramento de links de internet e infraestrutura hiperconvergente.

15. Normativos que disciplinam o serviço a ser contratado:

[Lei nº 14.133](#), de 1º de abril de 2021 - Lei de Licitações e Contratos Administrativos.

[Decreto nº 10.947](#), de 25 de janeiro de 2022 - Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

[Decreto nº 7.174](#), de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

[Instrução Normativa SGD/MGI nº 6](#) de 29 de março de 2023 - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

[Instrução Normativa SGD/ME nº 94](#) de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

[Instrução Normativa SLTI nº 01](#), de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

16. Do Acesso às Informações contidas nos presentes Estudos Preliminares:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que:

☒	As informações contidas nos presentes Estudos Preliminares DEVERÃO ESTAR DISPONÍVEIS para qualquer interessado, pois não se caracterizam como sigilosas.
☐	As informações contidas nos presentes Estudos Preliminares ASSUMEM CARÁTER SIGILOSOS , nos termos do Art. 23 da Lei nº 12.527/2011, e, portanto, deverão ter acesso restrito.
☐	

17. Equipe de Planejamento:

São responsáveis pela elaboração do presente documento que materializa os Estudos Preliminares da presente contratação os seguintes servidores:

Wekson José Barbieri Mariano Matrícula 87 Membro da Equipe de Planejamento	Elaine Leopoldino Ferreira Matrícula 198 Membro da Equipe de Planejamento	Vanessa Covre Rangel Marques Matrícula 140 Membro da Equipe de Planejamento



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 02/10/2025, às 16:39, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 03/10/2025, às 07:14, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 03/10/2025, às 16:29, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1021412** e o código CRC **6CE65D45**.



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

NLL - TERMO DE REFERENCIA DE TIC

Processo nº 9079618110000798.000048/2025-57

1. DEFINIÇÃO DO OBJETO

- 1.1. Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
- 1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.
- 1.3. O prazo de vigência da contratação é de 12 (doze) meses contados dos da assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.
- 1.3.1. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar;
- 1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual .

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

- 2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO

- 3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares

4. REQUISITOS DA CONTRATAÇÃO

4.1. Sustentabilidade

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.2. Garantia da contratação

4.2.1. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#), tendo em vista que o pagamento pelos serviços somente será realizado após a referida prestação e atesto pelo fiscal de contrato. Além disso, em caso de problema que se apresente posteriormente, o CRCES poderá instaurar procedimento administrativo sancionador com base na legislação vigente.

4.3. Vistoria

4.3.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo e-mail: administrativo@crc-es.org.br.

4.3.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

4.3.3. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.3.4. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.3.5. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.4. Local e horário da prestação dos serviços

4.4.1. Os serviços serão prestados na sede do CRCES, localizada na Rua Amélia da Cunha Ornelas, nº 30, Bairro Bento Ferreira, Vitória/ES – CEP: 29.050-620 Rotinas a serem cumpridas.

4.5. Materiais a serem disponibilizados

4.5.1. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário.

4.6. Informações relevantes para o dimensionamento da proposta

4.6.1. A Contratada deverá prestar serviços gerenciados de Tecnologia da Informação que abrangem o suporte técnico avançado (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a gestão de incidentes e mudanças. O escopo prevê a gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), com o fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, e a gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais. Será responsável também pelo monitoramento contínuo da infraestrutura, com identificação e mitigação proativa de riscos, pela manutenção preventiva e corretiva de todo o parque de TI, pela gestão e monitoramento dos links de internet, pela gestão e manutenção da infraestrutura hiperconvergente e do banco de dados em SQL Server. Além disso, inclui o fornecimento, instalação e gestão de um Firewall de Próxima Geração e a implementação e gestão de solução de backup local e em nuvem. Os serviços atenderão a única localidade do CRCES, até 60 estações de trabalho (físicas ou virtuais), 5 servidores físicos e 12 servidores virtuais.

4.6.2. A empresa contratada deverá estar plenamente capacitada para gerenciar toda a estrutura de TI híbrida do CRCES. Esta estrutura é complexa e inclui uma infraestrutura hiperconvergente (com

armazenamento baseado em Software-defined Storage - SDS), uma infraestrutura com acessos VDI (Virtual Desktop Infrastructure), máquinas virtuais e uma infraestrutura tradicional (com desktops físicos e notebooks).

4.6.3. A Contratada será responsável por assegurar a gestão completa dos backups e restores de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a disponibilidade e integridade dos dados em todas as plataformas.

4.7. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

4.7.1. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

4.8. Procedimentos de transição e finalização do contrato

4.8.1. Apresentar relatório final de atividades, contendo o resumo dos serviços executados, as ocorrências técnicas registradas, pendências identificadas e orientações para continuidade da operação da infraestrutura de TI, incluindo rede, segurança da informação, backup e suporte.

4.8.2. Entregar toda a documentação técnica e operacional produzida durante a execução do contrato, em meio físico e/ou digital, de forma organizada, classificada e atualizada, contemplando registros de configuração de equipamentos, scripts, inventários, diagramas de rede, manuais operacionais e demais documentos que garantam a rastreabilidade e integridade das informações

4.8.3. Transferir conhecimentos e informações relevantes ao(s) servidor(es) designado(s) pela Administração, por meio de reuniões técnicas, relatórios explicativos e capacitação operacional, com foco nos processos relacionados à infraestrutura de redes, segurança da informação, monitoramento e procedimentos de contingência

4.8.4. Assegurar a continuidade dos serviços durante eventual período de transição contratual, caso haja nova contratação em andamento, por prazo acordado com a Administração, a fim de garantir a operação ininterrupta dos serviços essenciais de tecnologia da informação.

4.8.5. Restituir, quando aplicável, equipamentos, materiais, documentos, credenciais, acessos a sistemas e demais bens disponibilizados pela contratante ao longo do contrato.

4.8.6. Emitir declaração formal de encerramento das obrigações contratuais, condicionada à aceitação pela fiscalização e à inexistência de pendências técnicas ou administrativas, comprovando a plena execução dos serviços contratados e a entrega dos produtos finais previstos. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

5. MODELO DE EXECUÇÃO DO OBJETO

5. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: 5 (cinco) dias da emissão da ordem de serviço;

5.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

5.1.3. Cronograma de realização dos serviços:

6. CARACTERÍSTICAS DA SOLUÇÃO:

6.1. ESTUDO DA SOLUÇÃO DE ACESSO VIA WI-FI.

6.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

6.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

6.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

6.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução.

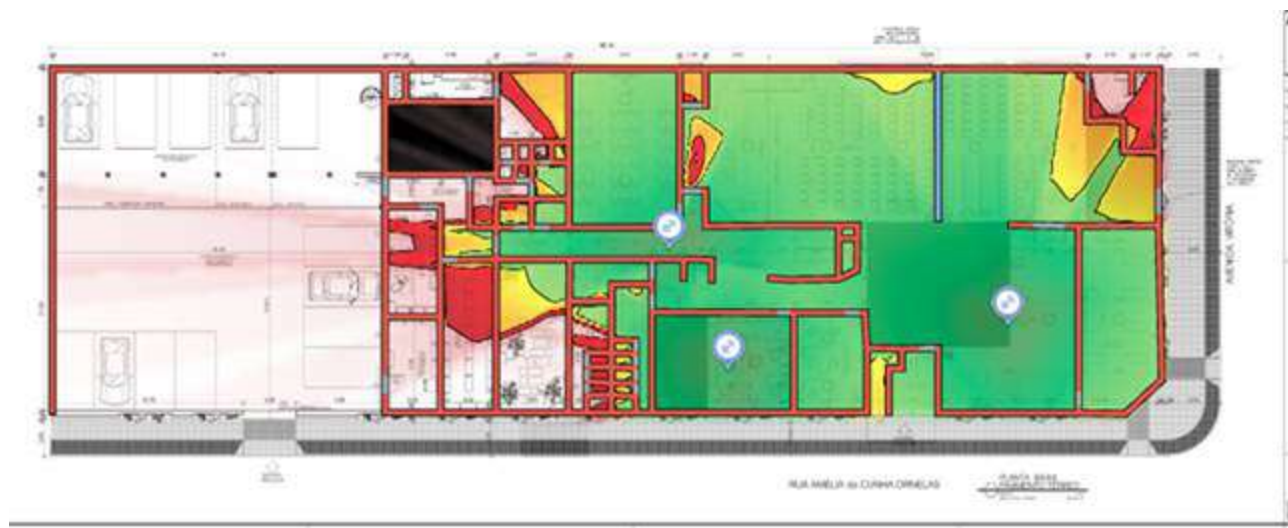
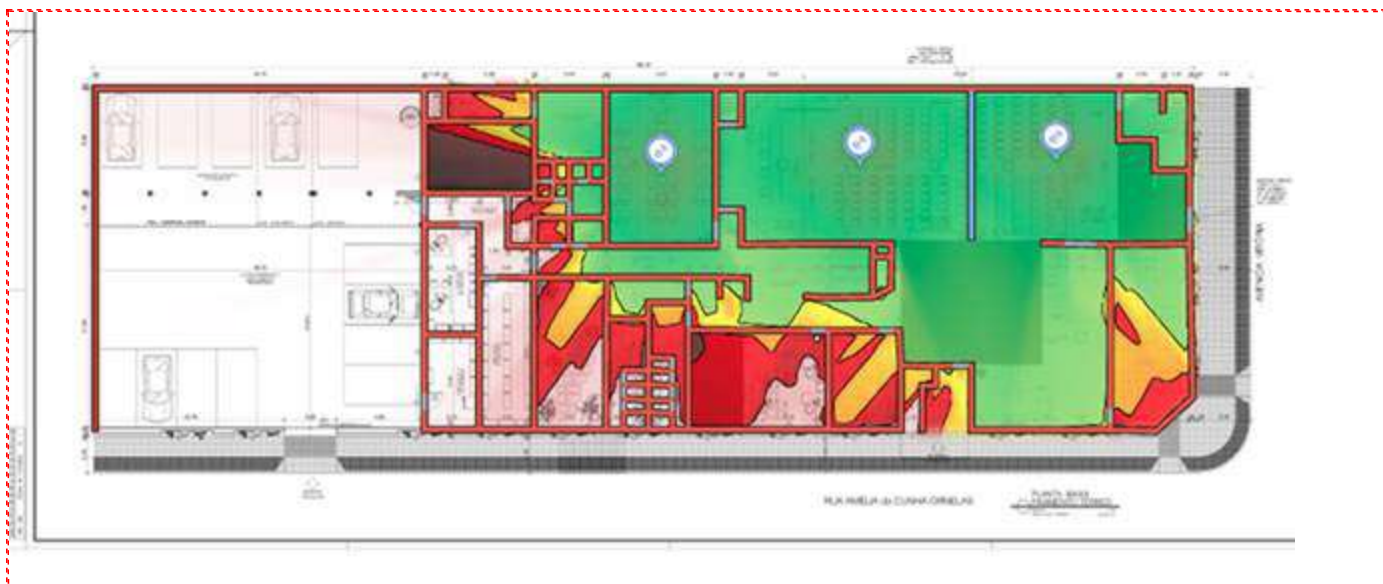
6.1.5. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

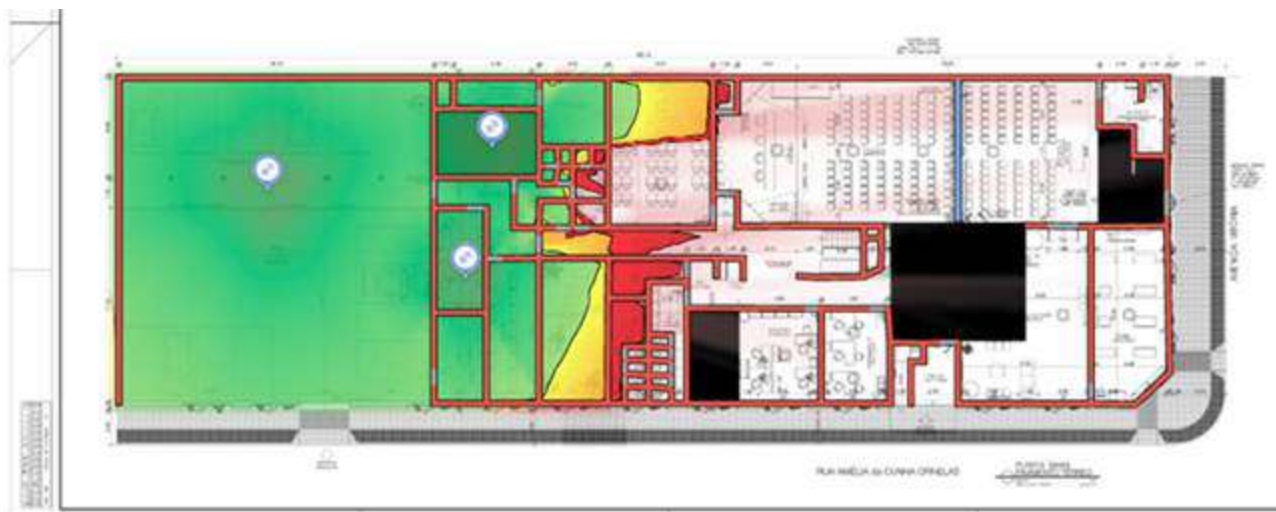
6.1.6. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.

6.2. Site Survey Preliminar

6.2.1. Para a definição da quantidade de equipamentos necessários, o CRCES realizou um levantamento de campo (site survey) preliminar, cujos resultados são apresentados a seguir:

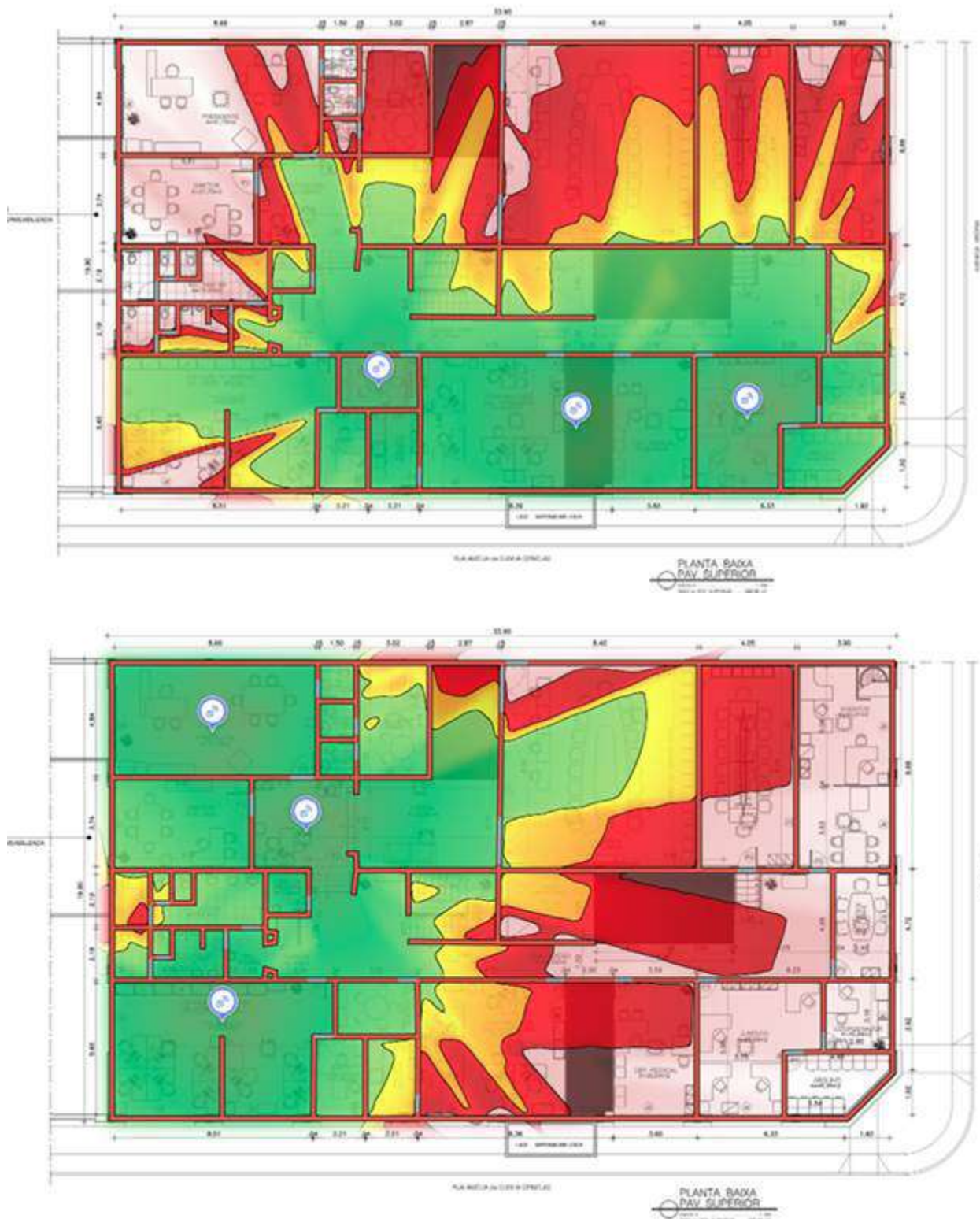
a) Pavimento térreo - 09 equipamentos





b) Pavimento superior - 09 equipamentos





6.2.2. ESTUDO DOS SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

6.2.2.1. Definição do objeto

6.2.2.2. Contratação de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial de acordo com a tabela abaixo:

TIPO	DESCRIÇÃO	QUANTIDADE
Virtualizador	Hyper-V	05
Servidor c/ Windows Server 2022	Dell PowerEdge R640	02
Servidor c/ Windows Server 2022	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01

Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01
Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados -VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01
Solução de acesso à internet via Wi-Fi	Conforme item 1 do Termo de referência	
Solução de segurança FWaaS	Conforme item 2 do Termo de referência	
Solução de backup Cooperativo	Conforme item 3 do Termo de referência	

7. Definição dos itens.

ITEM	SUBITEM	CATSER	DESCRIÇÃO	DESCRIÇÃO COMPLEMENTAR	UNIDADE DE MEDIDA	QUANTIDADE
01	01	30710	SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.	Fornecimento e instalação de uma rede corporativa Wi-Fi completa.	Mês	12
	02	30736	SOLUÇÃO DE SEGURANÇA FWaaS	Instalação e gestão de Firewall de Próxima Geração, conforme termo de referência.	Mês	12
	03	30744	SOLUÇÃO DE BACKUP CORPORATIVO	Implementação e de solução de backup local e em nuvem.	Mês	12
	04	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1,N2 E N3	Suporte técnico avançado (remoto e presencial) conforme termo de referência	Mês	12

8. Descrição técnica dos itens:

8.1. SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.

8.1.1. Características da solução

8.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

8.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

8.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

8.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

8.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

8.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.

8.1.2. Características dos pontos de acesso à internet via Wifi.

8.1.2.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

8.1.2.2. Deve ser compatível e gerenciado pelo equipamento que está incluso no ITEM “Solução de segurança FWaaS (Firewall como serviço). deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.1.2.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

8.1.2.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

8.1.2.5. Deve permitir ser gerenciado remotamente através de links WAN;

8.1.2.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

8.1.2.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

8.1.2.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

8.1.2.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

8.1.2.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

8.1.2.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

8.1.2.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

8.1.2.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

8.1.2.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

8.1.2.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

8.1.2.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

- 8.1.2.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
- 8.1.2.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 8.1.2.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 8.1.2.20. Deve permitir operação em modo Mesh;
- 8.1.2.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
- 8.1.2.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
- 8.1.2.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- 8.1.2.24. Deve suportar OFDMA;
- 8.1.2.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;
- 8.1.2.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 8.1.2.27. Deve suportar BSS Coloring;
- 8.1.2.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- 8.1.2.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;
- 8.1.2.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);
- 8.1.2.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;
- 8.1.2.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;
- 8.1.2.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
- 8.1.2.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 8.1.2.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
- 8.1.2.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- 8.1.2.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);
- 8.1.2.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
- 8.1.2.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.1.2.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 8.1.2.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 8.1.2.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

- 8.1.2.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.1.2.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 8.1.2.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 8.1.2.46. Deve implementar o padrão IEEE 802.11e;
- 8.1.2.47. Deve implementar o padrão IEEE 802.11h;
- 8.1.2.48. Deve implementar o padrão IEEE 802.3az;
- 8.1.2.49. Deve suportar ser gerenciado via SNMP;
- 8.1.2.50. Deve suportar consultas via REST API;
- 8.1.2.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
- 8.1.2.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
- 8.1.2.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- 8.1.2.54. Deve possuir indicadores luminosos (LED) para indicação de status;
- 8.1.2.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 8.1.2.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 8.1.2.57. Deve possuir certificado emitido pela Wi-Fi Alliance;
- 8.1.2.58. Deve estar homologado pela ANATEL na data de execução do pregão;
- 8.1.2.59. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.2.60. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.2.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.3. Características do equipamento controlador de pontos de acesso Wifi;

- 8.1.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 8.1.3.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
- 8.1.3.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- 8.1.3.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
- 8.1.3.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 8.1.3.6. Deve possuir 1 (uma) interface USB;
- 8.1.3.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);
- 8.1.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 8.1.3.9. Deve possuir tabela MAC com suporte a 32.000 endereços;
- 8.1.3.10. Deve operar com latência igual ou inferior à 1us (microsegundo);
- 8.1.3.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 8.1.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo

com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.1.3.13. Deve suportar a comutação de Jumbo Frames;

8.1.3.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

8.1.3.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

8.1.3.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.1.3.17. Deve implementar serviço de DHCP Relay;

8.1.3.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.1.3.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.1.3.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.1.3.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.1.3.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

8.1.3.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.1.3.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.1.3.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.1.3.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.1.3.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

8.1.3.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.1.3.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

8.1.3.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

8.1.3.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

8.1.3.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.1.3.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.1.3.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.1.3.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.1.3.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.1.3.37. Deve suportar MAC Authentication Bypass (MAB);

8.1.3.38. Deve implementar RADIUS CoA (Change of Authorization);

8.1.3.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

- 8.1.3.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 8.1.3.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
- 8.1.3.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 8.1.3.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 8.1.3.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 8.1.3.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 8.1.3.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 8.1.3.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 8.1.3.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 8.1.3.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 8.1.3.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 8.1.3.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 8.1.3.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 8.1.3.53. Deve permitir ser gerenciado através de IPv6;
- 8.1.3.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 8.1.3.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 8.1.3.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 8.1.3.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 8.1.3.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 8.1.3.59. Deverá suportar ser configurado e monitorado através de REST API;
- 8.1.3.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 8.1.3.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 8.1.3.62. Deve suportar temperatura de operação de até 45º Celsius;
- 8.1.3.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 8.1.3.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 8.1.3.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 8.1.3.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.3.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.3.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de

encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.4. Requisitos da instalação da solução de acesso à internet via Wi-Fi.

8.1.4.1. Implementação física.

8.1.4.1.1. Pontos de acesso:

8.1.4.1.1.1. Serviço de Implementação para rede WLAN8

8.1.4.1.1.2. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura 3 total, sendo observada a quantidade mínima estabelecida pela DTIC,

8.1.4.1.1.3. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;

8.1.4.1.1.4. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;

8.1.4.1.1.5. Requisitos gerais de Implantação

8.1.4.1.1.6. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.

8.1.4.1.1.7. Será realizada instalação física conforme a necessidade da contratante.

8.1.4.1.1.8. O ponto de acesso wifi deverá ser fixado no teto ou parede.

8.1.4.1.1.9. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

8.1.4.1.2. Controlador de pontos de acesso:

8.1.4.1.2.1. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;

8.1.4.1.2.2. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

8.1.4.1.3. Requisitos para instalação do cabeamento:

8.1.4.1.3.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;

8.1.4.1.3.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;

8.1.4.1.3.3. Conectorização e crimpagem dos cabos em ambos os extremos;

8.1.4.1.3.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;

8.1.4.1.3.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;

8.1.4.1.3.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;

8.1.4.1.3.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;

8.1.4.1.3.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

8.1.4.2. Implementação lógica.

8.1.4.2.1. Pontos de acesso:

8.1.4.2.1.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir

8.1.4.2.1.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

8.1.4.2.1.3. Cadastro das subscrições dos APs na plataforma de gerência;

8.1.4.2.1.4. Endereçamento e segmentação das Redes WIRELESS;

8.1.4.2.1.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e

policiamento de acordo com as aplicações a serem utilizadas na rede wireless);

- 8.1.4.2.1.6. Definição de políticas de bloqueio e permissão de acesso;
- 8.1.4.2.1.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.1.8. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.1.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 8.1.4.2.1.10. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.1.11. Configuração de Syslog, quando aplicável;
- 8.1.4.2.1.12. Configuração de redes locais (VLANs);
- 8.1.4.2.1.13. Configuração de redes locais (SSIDs);
- 8.1.4.2.1.14. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.1.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 8.1.4.2.1.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 8.1.4.2.1.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.18. Configurações de grupos de ponto de acesso;
- 8.1.4.2.1.19. Configuração de algoritmo de criptografia a ser utilizado;
- 8.1.4.2.1.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 8.1.4.2.1.22. Configuração de segurança de rede;
- 8.1.4.2.1.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 8.1.4.2.1.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 8.1.4.2.1.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;
- 8.1.4.2.1.26. Emissão de relatórios de implantação contendo:
- 8.1.4.2.1.27. Mapas de rede,
- 8.1.4.2.1.28. Relação de equipamentos implantados,
- 8.1.4.2.1.29. Configurações feitas nos softwares;
- 8.1.4.2.1.30. Resultado dos testes realizados;

8.1.4.2.2. Controlador de pontos de acesso:

- 8.1.4.2.2.1. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.2.2. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.2.3. Endereçamento IP;
- 8.1.4.2.2.4. Telnet, se necessário;
- 8.1.4.2.2.5. Secure Shell (SSH), se necessário;
- 8.1.4.2.2.6. Web (HTTP), se necessário;
- 8.1.4.2.2.7. Restrições (Filtros/ACLs) de Acesso;
- 8.1.4.2.2.8. Autenticação;
- 8.1.4.2.2.9. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.2.10. Configuração de redes locais (VLANs);
- 8.1.4.2.2.11. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.2.12. Configuração do protocolo Rapid Spanning Tree (RSTP);
- 8.1.4.2.2.13. Configuração de BPDU GUARD;
- 8.1.4.2.2.14. Configuração de Root Spanning Tree;
- 8.1.4.2.2.15. Interfaces de roteamento IP;
- 8.1.4.2.2.16. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;
- 8.1.4.2.2.17. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;
- 8.1.4.2.2.18. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.19. Otimização da Solução
- 8.1.4.2.2.20. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela

plataforma de gerenciamento unificado.

- 8.1.4.2.2.21. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.22. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;
- 8.1.4.2.2.23. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto
- 8.1.4.2.2.24. Ativação de recursos para o controle de broadcast storms;
- 8.1.4.2.2.25. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.26. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.27. Controle de acesso a rede através do padrão IEEE 802.1x;
- 8.1.4.2.2.28. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;
- 8.1.4.2.2.29. Configuração de DHCP Snooping;
- 8.1.4.2.2.30. Configuração de DHCP Relay;
- 8.1.4.2.2.31. Configuração de interface confiável (trust Interface);
- 8.1.4.2.2.32. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.
- 8.1.4.2.2.33. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;
- 8.1.4.2.2.34. Criação e ativação de regras de acesso e perfis de acesso à rede;
- 8.1.4.2.2.35. Configuração de parâmetros de qualidade de serviço (QoS);
- 8.1.4.2.2.36. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;
- 8.1.4.2.2.37. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;
- 8.1.4.2.2.38. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;
- 8.1.4.2.2.39. Ativação e teste das ACLs nos equipamentos fornecidos;
- 8.1.4.2.2.40. Homologação
- 8.1.4.2.2.41. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.
- 8.1.4.2.2.42. Documentação em formato PDF contendo os itens a seguir:
- 8.1.4.2.2.43. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.
- 8.1.4.2.2.44. Arquivos de configuração dos ativos de rede;
- 8.1.4.2.2.45. Backup das configurações dos softwares utilizados;
- 8.1.4.2.2.46. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega.

8.2. Solução de segurança FWaaS (Firewall como serviço).

8.2.1. Características da solução.

- 8.2.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
- 8.2.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
- 8.2.1.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
- 8.2.1.4. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
- 8.2.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o

pleno funcionamento da solução

8.2.1.6. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.2.1.7. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

8.2.1.8. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

8.2.2. Requisitos técnicos dos equipamentos que compõe a solução:

8.2.2.1. Características simplificadas:

8.2.2.1.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

8.2.2.1.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;

8.2.2.1.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;

8.2.2.1.4. Deve Suportar, no mínimo, 6,5 (Seis virgula cinco) Gbps de throughput VPN IPSec;

8.2.2.1.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;

8.2.2.1.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;

8.2.2.1.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;

8.2.2.1.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;

8.2.2.1.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.

8.2.2.1.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;

8.2.2.1.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;

8.2.2.1.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;

8.2.2.1.13. Deve possuir porta console RJ-45;

8.2.2.1.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;

8.2.2.1.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

8.2.2.1.16. Deve possuir Fontes redundantes.

8.2.2.1.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.

8.2.2.1.18. Deve ser licenciado para uso pelo período de duração do contrato.

8.2.2.1.19. Deve possuir garantia para uso pelo período de duração do contrato.

8.2.2.1.20. Firewalls de próxima geração (NGFW):

8.2.2.1.21. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

8.2.2.1.22. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

8.2.2.1.23. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8.2.2.1.24. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional

de todos os recursos;

8.2.2.1.25. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

8.2.2.1.26. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

8.2.2.2. Funcionalidades de rede e firewall:

8.2.2.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.2.2.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

8.2.2.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.2.2.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

8.2.2.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.2.2.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

8.2.2.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.2.2.2.8. Deverá suportar sFlow ou Netflow;

8.2.2.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.2.2.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

8.2.2.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.2.2.2.12. Deve implementar o protocolo ECMP;

8.2.2.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.2.2.2.14. Enviar log para sistemas de monitoração externos;

8.2.2.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

8.2.2.2.16. Deve possuir mecanismos de proteção anti-spoofing;

8.2.2.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

8.2.2.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

8.2.2.2.19. Suportar OSPF graceful restart;

8.2.2.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

8.2.2.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

8.2.2.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

8.2.2.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.2.2.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

8.2.2.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

8.2.2.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

8.2.2.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

8.2.2.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

8.2.2.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails,

notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

8.2.2.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

8.2.2.2.31. Deverá suportar controle por zonas de segurança;

8.2.2.2.32. Deverá suportar controles de políticas por porta e protocolo;

8.2.2.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.2.2.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.2.2.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.2.2.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.2.2.2.37. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.2.2.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.2.2.2.39. Suporte a objetos e regras IPV6;

8.2.2.2.40. Suporte a objetos e regras multicast;

8.2.2.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

8.2.2.2.42. Funcionalidade de controle de aplicações:

8.2.2.2.43. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

8.2.2.2.44. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.2.2.2.45. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

8.2.2.2.46. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

8.2.2.2.47. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

8.2.2.2.48. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

8.2.2.2.49. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

8.2.2.2.50. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

8.2.2.2.51. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

8.2.2.2.52. Identificar o uso de táticas evasivas via comunicações criptografadas;

8.2.2.2.53. Atualizar a base de assinaturas de aplicações automaticamente;

8.2.2.2.54. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

8.2.2.2.55. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

8.2.2.2.56. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

8.2.2.2.57. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de

aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

8.2.2.2.58. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

8.2.2.2.59. Deve alertar o usuário quando uma aplicação for bloqueada;

8.2.2.2.60. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.61. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.62. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

8.2.2.2.63. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.64. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

8.2.2.2.65. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

8.2.2.2.66. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

8.2.2.2.67. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

8.2.2.2.68. Funcionalidade de prevenção de intrusão de ameaças:

8.2.2.2.69. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

8.2.2.2.70. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.2.2.2.71. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.2.2.2.72. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e “quarentenar” IP do atacante por um intervalo de tempo;

8.2.2.2.73. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

8.2.2.2.74. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.2.2.2.75. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.2.2.2.76. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.2.2.2.77. Deve permitir o bloqueio de vulnerabilidades;

8.2.2.2.78. Deve permitir o bloqueio de exploits conhecidos;

8.2.2.2.79. Deve incluir proteção contra-ataques de negação de serviços;

8.2.2.2.80. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

8.2.2.2.81. Detectar e bloquear a origem de portscans;

8.2.2.2.82. Bloquear ataques efetuados por worms conhecidos;

8.2.2.2.83. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

8.2.2.2.84. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.2.2.2.85. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

8.2.2.2.86. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

8.2.2.2.87. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

8.2.2.2.88. Identificar e bloquear comunicação com botnets;

8.2.2.2.89. Registrar na console de monitoração as seguintes informações sobre ameaças

identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.2.2.2.90. Os eventos devem identificar o país de onde partiu a ameaça;

8.2.2.2.91. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

8.2.2.2.92. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

8.2.2.2.93. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

8.2.2.2.94. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

8.2.2.2.95. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

8.2.2.2.96. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

8.2.2.2.97. Funcionalidade de filtro de conteúdo web e dns:

8.2.2.2.98. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

8.2.2.2.99. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

8.2.2.2.100. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.2.2.2.101. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

8.2.2.2.102. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.2.2.2.103. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

8.2.2.2.104. Possuir pelo menos 70 (setenta) categorias de URLs;

8.2.2.2.105. Deve possuir a função de exclusão de URLs do bloqueio;

8.2.2.2.106. Permitir a customização de página de bloqueio;

8.2.2.2.107. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

8.2.2.2.108. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

8.2.2.2.109. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

8.2.2.2.110. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

8.2.2.2.111. Funcionalidade de identificação de usuários:

8.2.2.2.112. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

8.2.2.2.113. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

8.2.2.2.114. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

8.2.2.2.115. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários,

- suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 8.2.2.2.116. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.2.2.2.117. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 8.2.2.2.118. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 8.2.2.2.119. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 8.2.2.2.120. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 8.2.2.2.121. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 8.2.2.2.122. Funcionalidade de filtro de dados:
- 8.2.2.2.123. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 8.2.2.2.124. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.125. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.126. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
- 8.2.2.2.127. Funcionalidade de geolocalização:
- 8.2.2.2.128. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 8.2.2.2.129. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 8.2.2.2.130. Funcionalidade de vpn.
- 8.2.2.2.131. Suportar VPN Site-to-Site e Cliente-To-Site;
- 8.2.2.2.132. Suportar IPSec VPN;
- 8.2.2.2.133. A VPN IPSEC deve suportar 3DES;
- 8.2.2.2.134. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 8.2.2.2.135. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 8.2.2.2.136. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 8.2.2.2.137. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 8.2.2.2.138. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 8.2.2.2.139. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 8.2.2.2.140. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 8.2.2.2.141. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 8.2.2.2.142. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 8.2.2.2.143. Atribuição de DNS nos clientes remotos de VPN;
- 8.2.2.2.144. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 8.2.2.2.145. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 8.2.2.2.146. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 8.2.2.2.147. Deverá manter uma conexão segura com o portal durante a sessão;
- 8.2.2.2.148. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
- 8.2.2.2.149. Funcionalidade de qos, traffic shaping e priorização de tráfego;
- 8.2.2.2.150. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo,

(como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

8.2.2.2.151. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

8.2.2.2.152. Endereço de origem e Endereço de destino;

8.2.2.2.153. Usuário e grupo;

8.2.2.2.154. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.2.2.2.155. Por porta;

8.2.2.2.156. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

8.2.2.2.157. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

8.2.2.2.158. O QoS deve possibilitar a definição de fila de prioridade;

8.2.2.2.159. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

8.2.2.2.160. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

8.2.2.2.161. Suportar modificação de valores DSCP para o Diffserv;

8.2.2.2.162. Suportar priorização de tráfego usando informação de ToS (Type of Service);

8.2.2.2.163. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

8.2.2.2.164. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

8.2.2.2.165. Deve possibilitar a definição de bandas distintas para download e upload;

8.2.2.2.166. Funcionalidade de balanceamento inteligente de links;

8.2.2.2.167. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

8.2.2.2.168. A solução deve ser capaz de agregar vários links em uma interface virtual;

8.2.2.2.169. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

8.2.2.2.170. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

8.2.2.2.171. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

8.2.2.2.172. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

8.2.2.2.173. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

8.2.2.2.174. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

8.2.2.2.175. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

8.2.2.2.176. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

8.2.2.2.177. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface

está conectada;

8.2.2.2.178. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

8.2.2.2.179. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

8.2.2.2.180. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

8.2.2.2.181. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

8.2.2.2.182. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

8.2.2.2.183. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

8.2.2.2.184. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

8.2.2.2.185. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

8.2.2.2.186. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

8.2.2.2.187. A solução deve suportar nativamente conectores com clouds públicas;

8.2.2.2.188. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

8.2.2.2.189. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

8.2.2.2.190. Deve implementar balanceamento de link por hash do IP de origem;

8.2.2.2.191. Deve implementar balanceamento de link por hash do IP de origem e destino;

8.2.2.2.192. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

8.2.2.2.193. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

8.2.2.2.194. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

8.2.2.2.195. Funcionalidade de controlador de rede sem fio:

8.2.2.2.196. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

8.2.2.2.197. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

8.2.2.2.198. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

8.2.2.2.199. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

8.2.2.2.200. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

8.2.2.2.201. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de

canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

8.2.2.2.202. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

8.2.2.2.203. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

8.2.2.2.204. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.2.2.2.205. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.2.2.2.206. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.2.2.2.207. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

8.2.2.2.208. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

8.2.2.2.209. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

8.2.2.2.210. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.2.2.2.211. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.2.2.2.212. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

8.2.2.2.213. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

8.2.2.2.214. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

8.2.2.2.215. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

- 8.2.2.2.216. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 8.2.2.2.217. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 8.2.2.2.218. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 8.2.2.2.219. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 8.2.2.2.220. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 8.2.2.2.221. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 8.2.2.2.222. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.2.2.2.223. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 8.2.2.2.224. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 8.2.2.2.225. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
- 8.2.2.2.226. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 8.2.2.2.227. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 8.2.2.2.228. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
- 8.2.2.2.229. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
- 8.2.2.2.230. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
- 8.2.2.2.231. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
- 8.2.2.2.232. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;
- 8.2.2.2.233. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
- 8.2.2.2.234. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
- 8.2.2.2.235. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

- 8.2.2.2.236. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 8.2.2.2.237. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
- 8.2.2.2.238. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 8.2.2.2.239. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
- 8.2.2.2.240. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- 8.2.2.2.241. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.2.2.2.242. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 8.2.2.2.243. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 8.2.2.2.244. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 8.2.2.2.245. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 8.2.2.2.246. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 8.2.2.2.247. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 8.2.2.2.248. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 8.2.2.2.249. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 8.2.2.2.250. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 8.2.2.2.251. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 8.2.2.2.252. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 8.2.2.2.253. A solução deve permitir a configuração do captive portal com endereço IPv6;
- 8.2.2.2.254. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 8.2.2.2.255. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 8.2.2.2.256. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 8.2.2.2.257. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 8.2.2.2.258. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
- 8.2.2.2.259. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 8.2.2.2.260. A solução deve permitir que os usuários sejam capazes de acessar serviços

disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

8.2.2.2.261. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

8.2.2.2.262. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

8.2.2.2.263. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

8.2.2.2.264. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

8.2.2.2.265. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

8.2.2.2.266. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

8.2.2.2.267. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

8.2.2.2.268. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

8.2.2.2.269. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

8.2.2.2.270. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

8.2.2.2.271. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

8.2.2.2.272. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

8.2.2.2.273. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

8.2.2.2.274. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

8.2.2.2.275. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

8.2.2.2.276. A solução deve possuir ferramentas de diagnósticos e debug;

8.2.2.2.277. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

8.2.2.2.278. A solução deve suportar comunicação com elementos externos através de REST API;

8.2.2.2.279. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

8.2.2.2.280. Funcionalidade de controlador de rede cabeada:

8.2.2.2.281. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

8.2.2.2.282. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

8.2.2.2.283. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

8.2.2.2.284. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

8.2.2.2.285. Deve montar a topologia da rede de maneira automática;

8.2.2.2.286. Deve ser capaz de configurar os switches da rede;

8.2.2.2.287. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;

- 8.2.2.2.288. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 8.2.2.2.289. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 8.2.2.2.290. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 8.2.2.2.291. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 8.2.2.2.292. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 8.2.2.2.293. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard,;
- 8.2.2.2.294. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 8.2.2.2.295. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 8.2.2.2.296. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 8.2.2.2.297. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 8.2.2.2.298. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 8.2.2.2.299. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 8.2.2.2.300. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 8.2.2.2.301. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 8.2.2.2.302. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 8.2.2.2.303. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 8.2.2.2.304. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

8.2.3. Requisitos da instalação da Solução de segurança FWaaS (Firewall como serviço)

8.2.3.1. Implementação Física:

- 8.2.3.1.1. Levantamento de toda estrutura física do ambiente;
- 8.2.3.1.2. Levantamento da estrutura Elétrica;
- 8.2.3.1.3. Verificação do espaço a ser instalado os equipamentos;
- 8.2.3.1.4. Abertura e conferência das caixas dos equipamentos;
- 8.2.3.1.5. Fixação do equipamento no RACK;
- 8.2.3.1.6. Conexão da fonte de alimentação elétrica em réguas de tomada;
- 8.2.3.1.7. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;
- 8.2.3.1.8. Conexão das interfaces de rede com os switches;

8.2.3.2. Implementação lógica:

- 8.2.3.2.1. Parametrização do Licenciamento;
- 8.2.3.2.2. Parametrização das interfaces de rede;
- 8.2.3.2.3. Atualização da última versão de Firmware;
- 8.2.3.2.4. Parametrização das regras de NAT;
- 8.2.3.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 8.2.3.2.6. Parametrização de Controle de Aplicação;
- 8.2.3.2.7. Parametrização de VPN (Virtual Private Network);
- 8.2.3.2.8. Parametrização IDS/IPS;
- 8.2.3.2.9. Parametrização DNS;
- 8.2.3.2.10. Parametrização de Gateway Antivírus;

- 8.2.3.2.11. Parametrização de Objetos de Endereço;
- 8.2.3.2.12. Parametrização de Grupo de Objetos;
- 8.2.3.2.13. Parametrização de Load Balancing;
- 8.2.3.2.14. Parametrização de SSO (Single Sign-on);
- 8.2.3.2.15. Parametrização de SNMP;
- 8.2.3.2.16. Parametrização de NTP;
- 8.2.3.2.17. Parametrização de PortGroups;
- 8.2.3.2.18. Parametrização de Zones;
- 8.2.3.2.19. Parametrização de Serviços;
- 8.2.3.2.20. Parametrização de Rotas;
- 8.2.3.2.21. Parametrização de DHCP

8.3. SOLUÇÃO DE BACKUP CORPORATIVO

8.3.1. Características do Software de Backup

- 8.3.1.1. Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- 8.3.1.2. Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.
- 8.3.1.3. Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- 8.3.1.4. Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.
- 8.3.1.5. Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.
- 8.3.1.6. Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- 8.3.1.7. Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.
- 8.3.1.8. Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.
- 8.3.1.9. Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.
- 8.3.1.10. Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.
- 8.3.1.11. Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.
- 8.3.1.12. Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.
- 8.3.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações: O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.
- 8.3.1.14. Backup Incremental e Diferencial: Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.
- 8.3.1.15. Cópias de Backup Imutáveis: Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.
- 8.3.1.16. Retenção Personalizável: O software deve oferecer flexibilidade na configuração de políticas

de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.

8.3.1.17. Arquivamento Inteligente: Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.

8.3.1.18. Monitoramento e Alertas: O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.

8.3.1.19. Dashboard Intuitivo: Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.

8.3.1.20. Otimização de Recursos (IOPS e Throughput): O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.

8.3.1.21. Restauração Granular: Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.

8.3.1.22. Recuperação Bare-Metal: Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.

8.3.1.23. Testes de Restauração Automática: Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.

8.3.1.24. Integração Nativa com Provedores de Nuvem: Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.

8.3.1.25. Economia de Largura de Banda: Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.

8.3.1.26. Perfis de Acesso Personalizáveis: O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.

8.3.1.27. Controle de Acessos Granular: Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.

8.3.1.28. Suporte a LGPD e Outras Normas: O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.

8.3.1.29. Auditorias e Relatórios: Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.

8.3.1.30. Automatização de trabalhos de Backup: Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.

8.3.1.31. Integração com Ferramentas de Orquestração: Suporte para integração com ferramentas

8.3.1.32. de orquestração e automação (ex: scripts PowerShell, APIs).

8.3.1.33. Cobertura Completa: O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.

8.3.1.34. Recuperação Granular: Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.

8.3.1.35. Agendamento e Automação: A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

8.3.2. Características do backup local:

8.3.2.1. A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.

8.3.2.2. Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.

8.3.3. Características do backup em nuvem:

- 8.3.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.
- 8.3.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.
- 8.3.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.
- 8.3.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
- 8.3.3.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.
- 8.3.3.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.
- 8.3.3.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.
- 8.3.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.
- 8.3.3.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
- 8.3.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).
- 8.3.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.
- 8.3.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.
- 8.3.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.
- 8.3.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.
- 8.3.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.
- 8.3.3.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.
- 8.3.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.
- 8.3.3.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.
- 8.3.3.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.
- 8.3.3.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).
- 8.3.3.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.
- 8.3.3.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e

possíveis falhas.

8.3.3.23. Ferramentas de monitoramento nativas devem estar integradas.

8.3.3.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

8.3.4. Requisitos da instalação da Solução de Backup corporativo:

8.3.4.1. Implementação Física:

8.3.4.1.1. Verificar a estrutura elétrica do equipamento fornecido pelo CRC;

8.3.4.1.2. Verificar a conexão da fonte de alimentação elétrica em régua de tomada;

8.3.4.1.3. Verificar a conexão das interfaces de rede com os switches;

8.3.4.2. Implementação lógica.

8.3.4.2.1. Configurar o sistema de armazenamento local do equipamento, devendo:

8.3.4.2.1.1. Criar e configurar o arranjo de discos em RAID 5;

8.3.4.2.1.2. Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);

8.3.4.2.1.3. Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas; Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.

8.3.4.2.1. Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:

8.3.4.2.2.1. Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;

8.3.4.2.2.2. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

8.4. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

8.4.1. Definição do objeto

8.4.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, firewall, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

8.4.1.2. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21 da Lei nº 14.133, de 2021.

8.4.1.3. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

8.4.1.4. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

8.4.1.5. A contratada deverá:

8.4.1.5.1. Monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

8.4.1.5.2. Gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos

8.4.1.5.3. Possuir sistema de abertura de chamados pela internet.

8.4.1.5.4. Monitorar latência e uptime dos links configurados.

8.4.1.6. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

8.4.1.7. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela

empresa comprovando sua habilitação para a realização da vistoria.

8.4.2. Características do serviço prestado.

8.4.2.1. Monitoramento e suporte técnico:

- 8.4.2.1.1. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;
- 8.4.2.1.2. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:
- 8.4.2.1.3. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);
- 8.4.2.1.4. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;
- 8.4.2.1.5. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;
- 8.4.2.1.6. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

8.4.2.2. Serviços ambiente Legado:

8.4.2.2.1. Manutenção, gestão de ativos e rede:

- 8.4.2.2.1.1. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados na “Tabela do parque de informática do CRCES”;
- 8.4.2.2.1.2. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;
- 8.4.2.2.1.3. Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.
- 8.4.2.2.1.4. Executar a gestão técnica da infraestrutura de rede, abrangendo:
- 8.4.2.2.1.5. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;
- 8.4.2.2.1.6. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;
- 8.4.2.2.1.7. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;
- 8.4.2.2.1.8. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.
- 8.4.2.2.1.9. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

8.4.2.2.2. Serviços gerenciados:

- 8.4.2.2.2.1. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;
- 8.4.2.2.2.2. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;
- 8.4.2.2.2.3. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;
- 8.4.2.2.2.4. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

8.4.2.2.3. Controle, inventário e chamados:

- 8.4.2.2.3.1. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;
- 8.4.2.2.3.2. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

8.4.2.2.4. Logística e apoio à contratação:

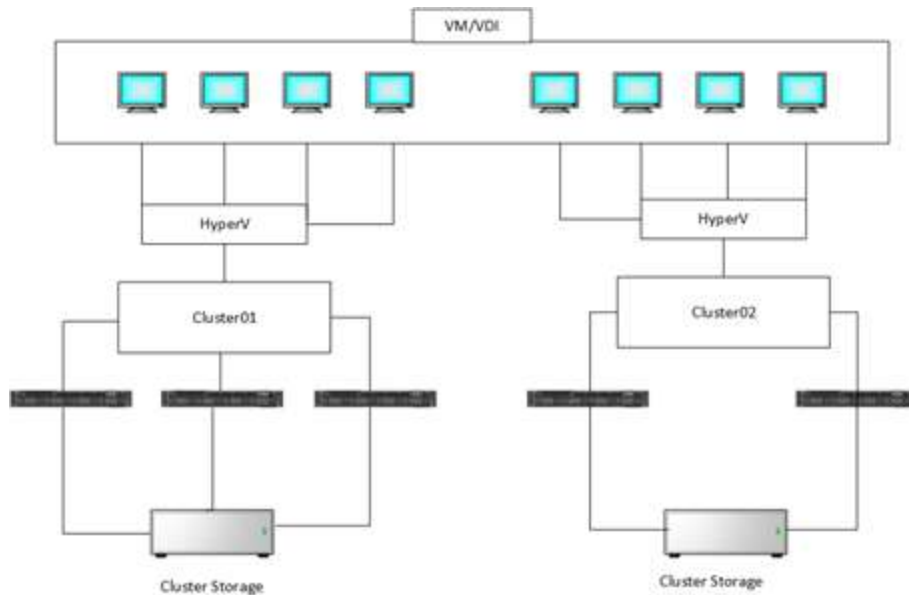
- 8.4.2.2.4.1. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;
- 8.4.2.2.4.2. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:
- 8.4.2.2.4.3. Elaboração de especificações técnicas;
- 8.4.2.2.4.4. Análise de propostas técnicas;
- 8.4.2.2.4.5. Apoio em processos licitatórios;
- 8.4.2.2.4.6. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

8.4.2.2.5. Atendimento presencial:

8.4.2.2.5.1. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 6 (seis) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

8.4.3. Tabela do parque de informática do CRCES:

8.4.3.1. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



8.4.4. Manutenção preventiva e corretiva.

8.4.4.1. Manutenção Preventiva:

8.4.4.1.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

8.4.4.1.2. Tais atividades incluem, mas não se limitam a:

8.4.4.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

8.4.4.1.2.2. Limpeza técnica interna e externa;

8.4.4.1.2.3. Aferição e calibração de dispositivos, quando aplicável;

8.4.4.1.2.4. Atualização de firmwares, BIOS e softwares;

8.4.4.1.2.5. Verificação e otimização de configurações;

8.4.4.1.2.6. Avaliação do desempenho geral e análise de logs;

8.4.4.1.2.7. Testes de funcionalidade e conectividade.

8.4.4.1.2.8. Realizar monitoramento contínuo do sistema de backup local, incluindo:

8.4.4.1.2.8.1. Acompanhamento da integridade dos discos e volumes lógicos;

8.4.4.1.2.8.2. Monitoramento do uso de espaço em disco e alertas proativos;

8.4.4.1.2.8.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

8.4.4.1.3. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.

8.4.4.1.4. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.

8.4.4.1.5. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.

8.4.4.1.6. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que

solicitado.

8.4.4.2. Manutenção Corretiva:

8.4.4.2.1. Em caso de surgimento de problema técnico em qualquer um dos equipamentos ou serviços listados no item de manutenção preventiva a contratada deverá providenciar laudo técnico e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.

8.4.4.2.2. CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.

8.4.4.2.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.

8.4.4.2.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.

8.4.4.2.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.

8.4.4.2.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 dias úteis após o recebimento dos novos equipamentos/peças.

8.4.4.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.

8.4.4.2.8. Durante a execução do serviço externo, a empresa contratada deverá:

8.4.4.2.9. Se responsabilizar pelo transporte dos equipamentos que serão retirados;

8.4.4.2.10. Providenciar termo de responsabilidade de retirada;

8.4.4.2.11. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

8.4.4.2.12. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;

8.4.4.2.13. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;

8.4.4.2.14. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;

8.4.4.2.15. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;

8.4.4.2.16. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto à qualidade do produto entregue;

8.4.4.2.17. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.

8.4.5.2. Suporte para o item 2 “SOLUÇÃO DE SEGURANÇA FWaaS”:

8.4.5.2.1. Serviço Continuado

8.4.5.2.1.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;

8.4.5.2.1.2. Efetuar toda rotina de backup das configurações semanalmente;

8.4.5.2.1.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

8.4.5.2.1.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

- 8.4.5.2.1.5. Atividades relativas à Solução de Segurança:
- 8.4.5.2.1.6. Criação das rotas para links.
- 8.4.5.2.1.7. Criação de NAT.
- 8.4.5.2.1.8. Liberação de portas.
- 8.4.5.2.1.9. Configuração do Filtro de Conteúdo.
- 8.4.5.2.1.10. Configuração do Controle de Aplicativos.
- 8.4.5.2.1.11. Configuração do Agente para autenticação LDAP.
- 8.4.5.2.1.12. Configuração para o Single Sign-On (SSO).
- 8.4.5.2.1.13. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 8.4.5.2.1.14. Configuração de VPN client to site.
- 8.4.5.2.1.15. Configuração de VPN site to site.
- 8.4.5.2.1.16. Criação de regras de Firewall.
- 8.4.5.2.1.17. Criação de regras de QoS.
- 8.4.5.2.1.18. Emitir relatório de segurança mensal por localidade.
- 8.4.5.2.1.19. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 8.4.5.2.1.20. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.
- 8.4.5.2.1.21. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

8.4.5.3. Suporte para o item 3 “SOLUÇÃO DE BACKUP CORPORATIVO”

8.4.5.3.1. Serviço Continuado

- 8.4.5.3.1.1. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:
- 8.4.5.3.1.2. Acompanhamento da integridade dos discos e volumes lógicos;
- 8.4.5.3.1.3. Monitoramento do uso de espaço em disco e alertas proativos;
- 8.4.5.3.1.4. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.
- 8.4.5.3.1.5. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:
- 8.4.5.3.1.6. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;
- 8.4.5.3.1.7. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).
- 8.4.5.3.1.8. Deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:
- 8.4.5.3.1.9. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;
- 8.4.5.3.1.10. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;
- 8.4.5.3.1.11. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;
- 8.4.5.3.1.12. Ajustar as políticas de backup e monitoramento para o novo ambiente.
- 8.4.5.3.1.13. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

8.4.5.4. SLA dos serviços e atendimento

- 8.4.5.4.1. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 8.4.5.4.2. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 8.4.5.4.3. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

8.4.5.4.4. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

8.4.5.4.5. Descrição de atendimento para cada nível de severidade:

8.4.5.4.5.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

8.4.5.4.5.2. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

8.4.5.4.5.2.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

8.4.5.4.5.2.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.4.5.3. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.3.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

8.4.5.4.5.3.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.4.5.4. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.4.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

8.4.5.4.5.4.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.5. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.5. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

8.4.5.4.5.6. Não poderá haver limites no quantitativo de abertura de chamados.

9. MODELO DE GESTÃO DO CONTRATO

9.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

9.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

9.4. O CRCES poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

9.5. Após a assinatura do contrato, o CRCES poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

9.6. Preposto

9.6.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

9.6.2. Fiscalização

9.6.3. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

9.6.4. O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

9.6.5. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

9.6.6. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

9.6.7. O fiscal do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

9.6.8. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

9.6.9. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

9.6.10. O fiscal do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

9.6.11. Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as

providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

9.6.12. Gestor do Contrato

9.6.13. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

9.6.14. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

9.6.15. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

9.6.16. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

9.6.17. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

9.6.18. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

9.6.19. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

10. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

10.1. A avaliação da execução do objeto utilizará o relatório/checklist para atesto de notas fiscais para aferição da qualidade da prestação do serviço.

10.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

10.1.1.1. não produzir os resultados acordados,

10.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

10.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

10.1.1.4. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

10.1.1.5. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

10.1.1.6. A avaliação da execução do objeto será conduzida utilizando o instrumento de verificação de conformidade, em conformidade com as especificações técnicas estabelecidas no item 5.

10.2. Do recebimento

10.2.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133, de 2021 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

10.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança

oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

10.2.3. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências. (Art. 22 e 23, X, Decreto nº 11.246, de 2022).

10.2.4. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

10.2.5. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

10.2.6. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

10.2.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

10.2.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

10.2.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as

10.2.10. especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

10.2.11. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

10.2.12. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

10.2.13. Emitir documento comprobatório da avaliação realizada pelos fiscais, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

10.2.14. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

10.2.15. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

10.2.16. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021 , comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

10.2.17. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

10.2.18. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

10.2.19. Liquidação

10.2.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de cinco dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

10.2.21. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

10.2.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

10.2.22.1. o prazo de validade;

10.2.22.2. a data da emissão;

10.2.22.3. os dados do contrato e do órgão contratante;

10.2.22.4. o período respectivo de execução do contrato;

10.2.22.5. o valor a pagar; e

10.2.22.6. eventual destaque do valor de retenções tributárias cabíveis.

10.2.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

10.2.24. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da

10.2.25. regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

10.2.26. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

10.2.27. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

10.2.28. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

10.2.29. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

10.2.30. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

10.3. Prazo de pagamento

10.3.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

10.4. Forma de pagamento

10.4.1. O pagamento será realizado preferencialmente por meio de chave pix indicada pelo fornecedor, desde que a conta para pagamento esteja em nome da empresa contratada, ou através de boleto/fatura emitido por este.

10.4.1.1. Na impossibilidade de pagamento via chave pix ou boleto/fatura, o valor poderá ser transferido para conta bancária, desde que a mesma esteja em nome da empresa contratada.

10.4.1.2. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

10.4.2. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

10.4.3. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

11.1. Forma de seleção e critério de julgamento da proposta.

11.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

11.2. Regime de execução

11.2.1. O regime de execução do objeto será empreitada por preço global.

11.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

11.3.1. Habilitação jurídica

11.3.1.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.3.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

11.3.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.4. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

11.3.1.5. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

11.3.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

11.3.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.3.1.9. Exigências Adicionais para Cooperativas

11.3.1.10. Caso a empresa participante seja uma cooperativa, deverá apresentar, além dos itens anteriores, a seguinte documentação complementar:

11.3.1.11. Relação de cooperados que atenderão o contrato, com atas de inscrição e comprovação de domicílio na localidade da sede da cooperativa.

11.3.1.12. Declaração de Regularidade de Situação do Contribuinte Individual (DRSCI) para cada um dos cooperados.

11.3.1.13. Comprovação do capital social proporcional ao número de cooperados necessários à execução do contrato.

11.3.1.14. Registro previsto na Lei nº 5.764, de 1971.

11.3.1.15. Comprovação de integração das quotas-partes dos cooperados que executarão o contrato.

11.3.1.16. Documentos de regularidade jurídica da cooperativa: ata de fundação, estatuto social, regimento dos fundos, editais e registros das últimas assembleias, além da ata que autorizou a participação na licitação.

11.3.1.17. Última auditoria contábil-financeira ou declaração de que a auditoria não foi exigida pelo órgão fiscalizador.

11.3.1.18. Modelo de gestão operacional, conforme a IN SEGES/ME nº 05/2017.

11.3.2. Habilitação fiscal, social e trabalhista

11.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

11.3.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.3.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.3.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.3.2.5. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.6. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.7. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

11.3.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.3.3. Qualificação Econômico-Financeira

11.3.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

11.3.4. Qualificação Técnica

Para a qualificação técnica, a empresa deverá cumprir os seguintes requisitos:

11.3.4.1. Requisitos de Capacidade Técnica da Empresa

11.3.4.1.1. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

11.3.4.1.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

- a) Serviços de backup em nuvem com, no mínimo, 25 terabytes de capacidade de armazenamento utilizável.
- b) Gestão de ambientes com infraestrutura virtualizada e VDI (Virtual Desktop Infrastructure) com pelo menos 30 estações virtuais.
- c) Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos.
- d) Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS).
- e) Hiperconvergência: Implementação, operação e manutenção de infraestruturas hiperconvergentes, com conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- f) Gerenciamento de Clusters de Servidores: Expertise em balanceamento de carga, otimização de recursos, failover e alta disponibilidade.
- g) Virtualização com Hyper-V: Conhecimento avançado em provisionamento, gerenciamento de imagens e otimização de desempenho de desktops virtuais.
- h) Administração de Banco de Dados SQL: Otimização de desempenho, segurança, backup e recuperação de desastres.
- i) Integração com Órgãos Governamentais: Experiência em integração de sistemas com a SEFAZ ES e o CFC, incluindo protocolos de comunicação e segurança.
- j) Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação para garantir alta disponibilidade.

11.3.4.1.2. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a

apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.

11.3.4.1.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

11.3.4.1.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

11.3.4.2. Qualificação Técnico-Profissional

11.3.4.2.1. Apresentação do(s) profissional(is), abaixo indicado(s), detentor(es) dos certificados abaixo indicado(s):

- a) Certificação em tecnologias de firewall e segurança de rede, como Fortinet, Palo Alto ou Cisco.
- b) ITIL v3 ou superior.
- c) MCSA Windows Server 2012 ou superior.
- d) Certificação para Instalação e Configuração de Switches DELL ou similar.

11.3.4.3. O(s) profissional(is) acima indicado(s) deverá(ão) participar do serviço objeto do contrato, e será admitida a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pela Administração (§ 6º do art. 67 da Lei nº 14.133, de 2021).

11.3.4.4. O profissional técnico indicado poderá ocupar a posição de diretor, sócio ou integrar o quadro permanente da licitante na condição de empregado ou de prestador de serviços, devendo ser comprovada sua vinculação com a licitante, até a data da apresentação dos documentos de habilitação, por meio de carteira de trabalho e previdência social (CTPS), contrato de prestação de serviços, ficha de registro de empregado ou contrato social, conforme o caso.

11.3.4.4.1 Será admitido a apresentação de Termo de Compromisso de contratação futura assinado pela licitante e pelo profissional indicado.

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado total da contratação é de R\$ 40.000,00 (quarenta mil reais) mensais, perfazendo o valor global de R\$ 480.000,00 (quatrocentos e oitenta mil reais) para o período contratual, conforme demonstrado na tabela abaixo. Ressalta-se que o valor foi apurado a partir da Pesquisa de Preços e consolidado no respectivo Mapa Comparativo de Preços, em conformidade com o disposto no inciso XXIII, alínea “i”, do art. 6º da Lei nº 14.133/2021.

ITEM 1					
SUBITEM	ESPECIFICAÇÕES	CATSER	QUANTIDADE	VALOR MENSAL	VALOR ANUAL
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	30710	12	R\$ 17.000,00	R\$ 204.000,00

2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	30736	12	R\$ 3.000,00	R\$ 36.000,00
3	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	30744	12	R\$ 8.000,00	R\$ 96.000,00
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo	30728	12	R\$ 12.000,00	R\$ 144.000,00

12.2 Para comprovar a conformidade técnica da proposta, a empresa deverá enviar no momento do envio da proposta:

- a) Documentação dos produtos ofertados: Catálogos, manuais, prospectos e outros documentos oficiais que permitam a clara identificação dos produtos. Esses documentos podem ser em português ou inglês, originais ou cópias. Não serão aceitos documentos criados especificamente para a licitação. A documentação pode ser entregue em formato eletrônico.
- b) Links de referência: Páginas da internet do fabricante do software, com indicação do endereço URL.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES.

13.2. A contratação será atendida pela seguinte dotação:

13.3. 6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

13.4. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação dos orçamentos pelo Conselho Federal de Contabilidade – CFC.

Wekson José Barbieri Mariano

Operador de Sistemas

Aprovo o Termo de Referência.

Encaminhe-se para as providências necessárias para a seleção do fornecedor, cumprindo as demais etapas legais para a contratação pública.

Contador **Walterleno Maifrede Noronha**
Presidente



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 03/10/2025, às 15:25, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 07/10/2025, às 16:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1021417** e o código CRC **E9BBDF7B**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

ANÁLISE DE RISCOS

Processo nº 9079618110000798.000048/2025-57

MAPA DE RISCOS – CONTRATAÇÃO

Nº	Risco Identificado	Probabilidade	Impacto	Consequência	Ações Preventivas	Ações Contingência	de	Responsável
1	Indisponibilidade de serviços críticos (rede, firewall, backup)	Média	Alto	Paralisação das atividades administrativas, perda de produtividade	Definir SLA rígido; monitoramento e relatórios de desempenho	Acionamento imediato do suporte presencial; uso de backup alternativo		Contratado + Fiscal do Contrato + CRCES
2	Falhas na gestão e manutenção do banco de dados SQL Server	Baixa	Alto	Perda ou inconsistência de dados estratégicos	Manutenção preventiva periódica; rotinas de backup testadas	Restauração a partir do backup; escalonamento para equipe especializada		Contratado
3	Atrasos no atendimento das demandas de suporte técnico	Média	Médio	Comprometimento do funcionamento de sistemas e serviços	Estabelecer prazos máximos no SLA; monitorar chamados	Redirecionar demandas urgentes para equipe interna até a solução		Contratado + CRCES

MAPA DE RISCOS – FORNECEDOR

Nº	Risco Identificado	Probabilidade	Impacto	Consequência	Ações Preventivas	Ações Contingência	de	Responsável
1	Fornecedor sem capacidade técnica ou equipe qualificada	Média	Alto	Execução inadequada dos serviços, falhas recorrentes	Exigir certificações e atestados; avaliar portfólio de contratos	Aplicar penalidades; acionar contrato emergencial/backup		Comissão de Licitação + Área Técnica + CRCES
2	Problemas financeiros/estruturais do fornecedor (continuidade)	Baixa	Médio	Interrupção do contrato antes do prazo	Exigir certidões fiscais e trabalhistas; análise de balanço	Substituição imediata por nova licitação; apoio de equipe interna		Comissão de Licitação + Jurídico + CRCES
3	Alta rotatividade de profissionais da equipe do fornecedor	Média	Médio	Perda de conhecimento técnico e queda na qualidade do serviço	Exigir cláusula de estabilidade mínima da equipe; acompanhamento da rotatividade	Solicitar substituição imediata de profissionais essenciais; reforço de equipe interna temporária		Contratado + Fiscal do Contrato



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 02/10/2025, às 16:52, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 03/10/2025, às 07:31, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 03/10/2025, às 16:29, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1021626** e o código CRC **9E6D5E48**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

Em atendimento ao Parecer Jurídico nº 94/2025, informamos que:

- **Recomendação 1:** A descrição do serviço comum já consta no item 1.2 do Termo de Referência. Considerando que o TR e o ETP são anexos do Edital, conclui-se que tais informações já integram automaticamente o próprio Edital.
- **Recomendação 2:** Ajustado o item 2.5.6, com a devida inclusão dos valores.
- **Recomendação 3:** A composição da equipe foi corrigida no ETP, com a inclusão das assinaturas faltantes e o ajuste do texto referente à qualificação técnica no item 11.3.4 do TR;
- **Recomendação 4:** O mapa de riscos foi adequado conforme a IN SEGES nº 5/2017.
- **Recomendação 5:** Inserida a menção ao mapa de preços no item 9.1 do TR.



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 03/10/2025, às 07:41, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Jorge Alexandre Fagundes registrado(a) civilmente como Jorge Alexandre Valdecir de Souza Fagundes, Usuário Externo**, em 07/10/2025, às 16:17, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1021652** e o código CRC **944E1EC7**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1021652



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

ANÁLISE Nº 32/2025/CRCES-CAF/CRCES-VPADM/CRCES-PRES/CRCES-CONSDIR/CRCES-
PLEN/CRCES

PROCESSO Nº 9079618110000798.000048/2025-57

ANEXO I – FORMULÁRIO DE SOLICITAÇÃO

Protocolo Administrativo nº 9079618110000798.000060/2025-61

Solicito que a despesa abaixo seja apreciada, discutida e deliberada.

1) Resumo do objeto: (Deve constar no DFD)

(☒)Sim (☐) Não:

Justificativa do interesse público para que a despesa seja realizada – (**Deve constar no ETP**)

(☒)Sim (☐) Não:

2) Valor total ou estimado: Deve constar no ETP e Termo de referência

(☒)Sim (☐) Não:

3) Dotação orçamentária: Deve constar no ETP e Termo de referência

3.1) Conta Contábil (☒)Sim (☐) Não:

3.2) Projeto (☒)Sim (☐) Não:

3.3) Previsão PCA (☒)Sim (☐) Não:

4) Nos itens que compõe o planejamento da licitação são estabelecidos os parâmetros essenciais para a contratação. De forma geral o processo enviado atende aos requisitos legais sobre a fase

preparatória exigidos na LEI 14.133/2021 no artigo 18: [L14133 \(planalto.gov.br\)](https://planalto.gov.br)

DFD (x)Sim () Não:

ETP (x)Sim () Não:

Mapa de Riscos (x)Sim () Não:

TR (x)Sim () Não:

EM CASOS DE CONTRATAÇÕES ENQUADRADAS PELA RESOLUÇÃO CRCES Nº 481, DE 24 DE ABRIL 2024

Declaração de aprovação emitida pela Câmara de Administração e Finanças - CAF, atestando a possibilidade da contratação por dispensa de licitação, sem a necessidade de análise jurídica, em conformidade com a RESOLUÇÃO CRCES Nº 481, DE 24 DE ABRIL DE 2024.

Não se Aplica

Observações:



Documento assinado eletronicamente por **Mário Zan Barros, Conselheiro**, em 18/09/2025, às 13:29, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1026621** e o código CRC **44AAA14B**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

Ao Setor de Controle Interno,

Encaminhe-se o presente processo para **análise da regularidade e verificação do atendimento às recomendações jurídicas** previamente emitidas.

Após manifestação, devolver para prosseguimento.



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 06/10/2025, às 08:09, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1051412** e o código CRC **27CFB0A4**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1051412

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

Processo nº 9079618110000798.000048/2025-57

Ao Administrativo

Em atenção ao Despacho nº 1051412, informo que, após análise, verifico que as providências indicadas no Parecer Jurídico nº 094/2025 (1021378) foram atendidas parcialmente, conforme segue:

Recomendação 1

Análise do Controle Interno: A recomendação foi atendida parcialmente, visto que foi acostado aos autos o Termo de Referência com a alteração recomendada. Assim, considera-se a recomendação atendida somente após o ajuste do Edital.

Recomendação 2

Análise do Controle Interno: A recomendação foi atendida com a inclusão do valor, conforme verificado no item 6.7. Importante informar que os itens foram reorganizados e revisados pela área responsável, e o item objeto da recomendação passou de 2.5 para 6.7. Assim, o Controle Interno entende que a recomendação jurídica foi atendida, devendo apenas ser assegurada a efetiva incorporação das diretrizes do Despacho SEI nº 0942432 nos documentos da contratação (Edital e Termo de Referência), de forma a garantir a segurança jurídica do processo e a observância dos princípios da Administração Pública.

Recomendação 3

Análise do Controle Interno: A recomendação foi atendida.

Recomendação 4

Análise do Controle Interno: A recomendação foi atendida.

Recomendação 5

Análise do Controle Interno: A recomendação foi atendida, conforme verificado no item 12.1. Importante informar que os itens foram reorganizados e revisados pela área responsável, e o item objeto da recomendação passou de 9.1 para 12.1.

Demais constatações realizadas na conferência dos documentos:

- No ETP, o item 2.1.1 “Justificativa” encontra-se em branco (retirar ou preencher);
- O item 3.1.1 “Serviços Continuados” está com o texto desconfigurado.

Encaminhe-se o processo ao Setor Administrativo para adoção das medidas complementares e posterior comprovação do atendimento integral das recomendações.

Atenciosamente,

Leandra Machado

Controller CRCES



Documento assinado eletronicamente por **Leandra Machado, Controladora**, em 06/10/2025, às 10:54, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1052010** e o código CRC **4D40A39E**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1052010

ESTUDO TÉCNICO PRELIMINAR

Processo nº 9079618110000798.000048/2025-57

ESTUDOS PRELIMINARES

O presente documento visa analisar a viabilidade da presente contratação, bem como levantar os elementos essenciais que servirão para compor o Termo de Referência ou projeto Básico, de forma a melhor atender às necessidades da Administração.

Dados do Processo:

Órgão Responsável pela Contratação:	Conselho Regional de Contabilidade do Espírito Santo.
Objeto:	Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
Nº do Processo Administrativo:	9079618110000798.000048/2025-57

1. Justificativa para a Contratação Conjunta de Serviços de Tecnologia da Informação:

1.1. Introdução

O presente estudo tem como objetivo fundamental apresentar a justificativa técnica e legal para a contratação conjunta de diversos serviços de Tecnologia da Informação (TI) pelo Conselho Regional de Contabilidade do Espírito Santo (CRCES). A decisão por uma contratação unificada, em detrimento da fragmentação em múltiplos contratos, fundamenta-se em princípios basilares da administração pública, notadamente a economicidade, a eficiência, a segurança jurídica e a busca pela solução mais vantajosa para a Administração, em consonância com as diretrizes estabelecidas pela Lei nº 14.133/21.

A infraestrutura de TI do CRCES, conforme detalhado ao longo deste documento, é um pilar essencial para a continuidade e a qualidade dos serviços prestados à sociedade e à classe contábil. A complexidade e a interdependência dos serviços de Wi-Fi corporativo, backup, suporte técnico e firewall demandam uma abordagem integrada para garantir a robustez, a segurança e a disponibilidade dos sistemas críticos. A contratação isolada de cada um desses componentes não apenas eleva os riscos operacionais, mas também compromete a gestão eficiente e a otimização dos recursos públicos.

Este texto abordará os aspectos técnicos e jurídicos que sustentam a opção pela contratação conjunta, destacando os benefícios em termos de economicidade, a mitigação de problemas inerentes à multiplicidade de prestadores de serviços e a conformidade com a legislação vigente, em especial a Lei nº 14.133/2021 e as melhores práticas de contratação de soluções de TI para a Administração Pública.

1.2. Da Necessidade da Contratação e a Interdependência dos Serviços de TI

O Conselho Regional de Contabilidade do Espírito Santo (CRCES) reconhece a Tecnologia da Informação como um elemento estratégico e indispensável para o cumprimento de sua missão institucional. A atual infraestrutura de TI, embora funcional, enfrenta desafios significativos que justificam a presente contratação. Conforme o documento de Estudos Preliminares, o CRCES dispõe de apenas um funcionário técnico especializado em TI, o que resulta em sobrecarga de trabalho e na impossibilidade de atender a todas as demandas operacionais e administrativas complexas, como a manutenção de servidores, gestão de incidentes, monitoramento contínuo de redes, implementação de políticas de segurança da informação e suporte técnico especializado. Adicionalmente, a rede cabeada existente apresenta falhas que impactam diretamente a conectividade e a produtividade da instituição.

A contratação em questão visa suprir essas lacunas e fortalecer a infraestrutura de TI do CRCES, abrangendo os seguintes serviços essenciais e interdependentes:

•**Solução de Acesso via Wi-Fi:** Fundamental para garantir conectividade de alta qualidade e superar as limitações da rede cabeada atual,

promovendo a mobilidade e a eficiência no ambiente de trabalho.

•**Firewall de Próxima Geração:** Crucial para fortalecer a segurança da rede, proteger os dados do CRCES contra ameaças cibernéticas e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

•**Serviços Continuados de Suporte (N1, N2 e N3):** Essenciais para a manutenção da infraestrutura tecnológica, garantia do funcionamento adequado dos sistemas críticos, gestão de incidentes e mudanças, e monitoramento contínuo da infraestrutura.

•**Backup Corporativo (Local e em Nuvem):** Indispensável para assegurar a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, garantindo a continuidade dos negócios e a conformidade com a LGPD.

A natureza desses serviços é intrinsecamente interligada. A eficácia de um sistema de backup, por exemplo, depende diretamente da segurança da rede (Firewall) e da capacidade de suporte técnico para gerenciar eventuais falhas. Da mesma forma, a qualidade da conectividade Wi-Fi impacta a performance de todas as aplicações e serviços que trafegam pela rede. A contratação fragmentada desses serviços, com diferentes prestadores, geraria uma série de desafios e riscos que serão detalhados nas seções seguintes, comprometendo a eficiência e a segurança da infraestrutura de TI do CRCES.

1.3. Arcabouço Legal: A Lei nº 14.133/2021 e os Princípios da Contratação Pública

A Nova Lei de Licitações e Contratos Administrativos, Lei nº 14.133, de 1º de abril de 2021, trouxe inovações significativas para o processo de contratação pública no Brasil, com o objetivo de modernizar, otimizar e tornar mais eficientes as aquisições e contratações realizadas pela Administração Pública. Em seu Art. 5º, a Lei elenca uma série de princípios que devem nortear a aplicação da norma, dentre os quais se destacam a economicidade, a eficiência, o interesse público, o planejamento, a transparência, a segurança jurídica e a vantajosidade. Estes princípios são pilares para a justificativa da contratação conjunta dos serviços de TI.

A Lei nº 14.133/2021, ao contrário da legislação anterior, enfatiza a busca pela solução mais vantajosa para a Administração, que não se restringe apenas ao menor preço, mas considera a relação custo-benefício, a qualidade, a inovação e a sustentabilidade. A contratação conjunta de serviços de TI, quando devidamente justificada, alinha-se perfeitamente a essa premissa, pois permite uma visão sistêmica e integrada da infraestrutura, otimizando recursos e minimizando riscos.

Embora a Lei nº 14.133/2021 defina a 'contratação integrada' especificamente para obras e serviços de engenharia (Art. 6º, XXXII), o conceito subjacente de agrupar itens interdependentes para obter maior eficiência e vantajosidade pode ser analogicamente aplicado à contratação de serviços de TI. A Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que disciplina as contratações de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades do SISP, reforça a importância do planejamento e da busca por soluções que atendam às necessidades de forma abrangente e eficiente.

O Estudo Técnico Preliminar (ETP), conforme previsto na Lei nº 14.133/2021 e detalhado na IN SGD/ME Nº 94/2022, é o documento fundamental que embasa a decisão pela contratação. Ele deve contemplar a análise comparativa de soluções e custos, a estimativa do custo total da

contratação e a declaração da viabilidade da contratação. A presente justificativa, ao demonstrar os benefícios da contratação conjunta, serve como subsídio para o ETP, evidenciando que a opção por um único prestador para os serviços de Wi-Fi, backup, suporte e firewall é a que melhor atende aos princípios da Lei e às necessidades do CRCES.

Outro ponto relevante é a Matriz de Alocação de Riscos, que se torna ainda mais crucial em contratações complexas como a de serviços de TI. A Lei nº 14.133/2021 exige a definição clara de riscos e responsabilidades entre as partes. Em uma contratação conjunta, a alocação de riscos é simplificada, pois a responsabilidade pela integração e funcionamento dos diversos componentes recai sobre um único fornecedor, facilitando a gestão e a resolução de eventuais problemas.

1.4. Economicidade e Vantagens da Contratação Conjunta

A busca pela economicidade é um dos princípios fundamentais que regem as contratações públicas, conforme expresso no Art. 5º da Lei nº 14.133/2021. A contratação conjunta dos serviços de TI, em vez de licitações separadas para cada item (Wi-Fi, backup, suporte e firewall), representa uma estratégia que maximiza a eficiência na aplicação dos recursos públicos e gera uma série de vantagens econômicas e operacionais para o CRCES.

Primeiramente, a contratação de um único fornecedor para a gestão integrada de múltiplos serviços de TI permite a obtenção de economias de escala. Ao consolidar a demanda, o CRCES ganha maior poder de negociação, o que pode resultar em propostas mais competitivas e preços unitários mais vantajosos para cada serviço. A diluição de custos administrativos e operacionais do fornecedor em um contrato de maior escopo tende a refletir em um custo total da contratação mais baixo para a Administração Pública.

Além disso, a contratação conjunta simplifica os processos administrativos e burocráticos. A gestão de um único contrato, em comparação com a gestão de múltiplos contratos, reduz significativamente a carga de trabalho da equipe interna do CRCES, liberando recursos humanos para outras atividades estratégicas. Isso se traduz em economia de tempo e, consequentemente, de recursos financeiros, uma vez que menos horas de trabalho são dedicadas à fiscalização e acompanhamento de diversos contratos.

A otimização dos recursos também se manifesta na redução de custos indiretos. A coordenação entre diferentes fornecedores, a resolução de conflitos de responsabilidade e a necessidade de interface entre sistemas distintos geram custos ocultos e ineficiências. Com um único prestador, esses custos são minimizados, pois a responsabilidade pela integração e pelo funcionamento harmonioso de toda a infraestrutura de TI recai sobre uma única empresa, que possui o conhecimento global do ambiente e a capacidade de gerenciar as interdependências de forma proativa.

Por fim, a contratação conjunta contribui para a previsibilidade orçamentária. Com um contrato abrangente, o CRCES tem uma visão mais clara e consolidada dos custos totais envolvidos na manutenção e gestão de sua infraestrutura de TI, facilitando o planejamento financeiro e a alocação de recursos de forma mais eficiente ao longo do tempo. Essa previsibilidade é essencial para uma gestão pública responsável e transparente.

1.5. Mitigação de Problemas e Impactos Negativos da Multiplicidade de Prestadores

A contratação fragmentada de serviços de Tecnologia da Informação, com a pulverização de responsabilidades entre múltiplos prestadores, embora possa parecer, à primeira vista, uma estratégia de diversificação, acarreta uma série de problemas e impactos negativos que comprometem a eficiência, a segurança e a continuidade das operações do CRCES. A experiência demonstra que a gestão de diversos contratos para serviços interdependentes de TI pode gerar complexidades e vulnerabilidades que superam quaisquer supostas vantagens.

Um dos principais desafios reside na incompatibilidade e nas falhas de integração entre os diferentes sistemas e equipamentos fornecidos por empresas distintas. A infraestrutura de TI do CRCES, conforme descrito, é híbrida e complexa, envolvendo soluções de Wi-Fi, backup, suporte e firewall, além de infraestrutura hiperconvergente, acessos VDI, máquinas virtuais e desktops físicos. A falta de um gerenciamento unificado pode levar a problemas de interoperabilidade, dificultando a comunicação entre os componentes e resultando em falhas operacionais, interrupções de serviço e degradação da performance geral do ambiente. A identificação da causa raiz de um problema torna-se um processo moroso e dispendioso, pois cada fornecedor pode atribuir a falha ao outro, criando um cenário de “empurra-empurra” de responsabilidades.

A dificuldade na gestão e fiscalização contratual é outro impacto negativo significativo. A multiplicidade de contratos implica na necessidade de gerenciar diferentes prazos, escopos, níveis de serviço (SLAs) e pontos de contato. Isso sobrecarrega a equipe interna do CRCES, que já é reduzida, desviando seu foco de atividades estratégicas para a burocracia administrativa. A fiscalização torna-se mais complexa, exigindo um esforço desproporcional para garantir que cada fornecedor esteja cumprindo suas obrigações de forma isolada, sem uma visão integrada do impacto no ambiente como um todo.

A diluição da responsabilidade é um risco inerente à contratação fragmentada. Em caso de incidentes de segurança, falhas de sistema ou perda de dados, a apuração do responsável pela falha e a consequente aplicação de sanções contratuais tornam-se extremamente difíceis. Essa incerteza jurídica pode atrasar a resolução de problemas críticos, gerar prejuízos financeiros e de imagem para o CRCES, e comprometer a conformidade com regulamentações como a LGPD. Com um único prestador, a responsabilidade pela integridade e funcionamento de toda a infraestrutura é centralizada, facilitando a governança e a responsabilização.

Adicionalmente, a fragmentação pode levar a custos elevados e ineficiências operacionais. A ausência de uma visão consolidada da infraestrutura impede a otimização de recursos e a identificação de redundâncias ou gargalos. Cada fornecedor pode operar de forma isolada, sem considerar o impacto de suas ações no ambiente geral, o que pode resultar em investimentos desnecessários ou na subutilização de ativos. A falta de padronização e a necessidade de múltiplas interfaces de comunicação entre os fornecedores também contribuem para o aumento dos custos operacionais.

Por fim, a vulnerabilidade de segurança é amplificada em um ambiente com múltiplos prestadores. A gestão de segurança da informação exige uma abordagem holística e integrada. A fragmentação pode criar brechas e pontos cegos, dificultando a implementação de políticas de segurança consistentes e a resposta rápida a ameaças cibernéticas. Um único fornecedor, com uma visão abrangente da infraestrutura, está em melhor posição para implementar e gerenciar soluções de segurança de forma eficaz, garantindo a proteção dos dados e sistemas do CRCES.

Diante desses riscos e impactos negativos, a contratação conjunta de serviços de TI emerge como a solução mais prudente e vantajosa para o CRCES, garantindo a sinergia entre os serviços, a otimização da gestão, a clareza na alocação de responsabilidades e a segurança da infraestrutura tecnológica.

1.6. Conclusão

Diante do exposto, a contratação conjunta dos serviços de Tecnologia da Informação para o Conselho Regional de Contabilidade do Espírito Santo (CRCES), abrangendo Wi-Fi corporativo, backup, serviços de suporte e firewall, configura-se como a abordagem mais estratégica, eficiente e em conformidade com os preceitos da Lei nº 14.133/2021. Esta modalidade de contratação não apenas otimiza a aplicação dos recursos públicos, mas também mitiga os riscos inerentes à fragmentação de serviços interdependentes, garantindo a continuidade, a segurança e a qualidade da infraestrutura de TI do órgão.

A centralização da responsabilidade em um único prestador de serviços especializados em TI proporciona uma gestão mais simplificada e eficaz, com clareza na alocação de responsabilidades e maior agilidade na resolução de problemas. A economicidade é alcançada por meio de ganhos de escala, redução de custos administrativos e operacionais, e maior previsibilidade orçamentária. Adicionalmente, a abordagem integrada fortalece a segurança da informação, minimizando vulnerabilidades e garantindo a conformidade com a legislação vigente, como a LGPD.

Em suma, a contratação conjunta é a solução que melhor atende ao interesse público, promovendo a eficiência, a economicidade e a segurança jurídica, pilares da boa gestão pública. Recomenda-se, portanto, a continuidade do processo licitatório sob esta perspectiva integrada, visando a obtenção da proposta mais vantajosa e a garantia de uma infraestrutura de TI robusta e confiável para o CRCES.

2. Diretrizes gerais para a contratação:

2.1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERADO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INT PÚBLICO;

O **Conselho Regional de Contabilidade do Espírito Santo (CRCES)** desempenha um papel essencial na sociedade, oferecendo serviços como fiscalização e registro do exercício profissional, orientação técnica e promoção de desenvolvimento profissional da classe contábil. A execução eficiente dessas atividades depende diretamente de uma **infraestrutura de Tecnologia da Informação (TI)** robusta, segura e eficaz, capaz de atender às crescentes demandas internas e externas e garantir a proteção de dados sensíveis, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**.

Atualmente, o CRCES conta com apenas **um servidor técnico especializado em TI**, o qual se encontra sobrecarregado com demandas operacionais, administrativas e técnicas. Essa limitação compromete a execução de atividades críticas e complexas, como:

- Manutenção de servidores e redes;
- Monitoramento contínuo da infraestrutura;
- Gestão de incidentes e mudanças;
- Suporte técnico especializado;
- Implementação de políticas de segurança da informação.

Além disso, a **infraestrutura de rede cabeada apresenta falhas recorrentes**, impactando diretamente a conectividade e a produtividade das equipes. A segurança da informação também requer reforços, com a **adoção de soluções modernas e eficazes contra ameaças cibernéticas**.

Atualmente, o CRCES mantém o **Contrato Administrativo nº 40/2024**, firmado com a empresa Smart Fusion Technology Ltda, com vigência até 15/12/2025. Contudo, trata-se de contrato emergencial, **sem possibilidade de prorrogação**, o que torna **necessária a realização de novo procedimento licitatório**, a fim de garantir a contratação regular e contínua dos serviços especializados de gerenciamento de TI.

A nova contratação tem como objetivo **assegurar a continuidade, eficiência e segurança das operações tecnológicas do CRCES**, por meio da prestação dos seguintes serviços especializados:

- Suporte técnico avançado para a infraestrutura tecnológica;
- Manutenção preventiva e corretiva de servidores e redes;
- Gestão de incidentes e implementação de melhorias;
- Monitoramento proativo da infraestrutura de TI;

- Fornecimento, instalação e gestão de **rede Wi-Fi corporativa**;
- Implantação e gestão de **Firewall de Próxima Geração**;
- Implementação e gerenciamento de **solução de backup híbrida** (local e em nuvem), conforme exigências da LGPD.

Além disso, a contratação visa **reduzir a sobrecarga do único servidor de TI**, promovendo maior eficiência e qualidade dos serviços prestados pelo Conselho à sociedade e à classe contábil.

Natureza do Objeto – Serviço Comum e Continuado

O objeto desta contratação caracteriza-se como **serviço comum**, nos termos do inciso II do art. 6º da **Lei nº 14.133/2021**, por poder ser descrito de forma objetiva e padronizada, sem necessidade de especificações técnicas complexas ou qualificações exclusivas. São serviços amplamente ofertados no mercado, com condições técnicas e comerciais similares entre fornecedores.

Trata-se, ainda, de **serviço de natureza continuada**, tendo em vista a sua **necessidade permanente e ininterrupta**, indispensável à execução das atividades finalísticas do CRCES. A descontinuidade desses serviços comprometeria a segurança da informação, a funcionalidade dos sistemas internos e a continuidade do atendimento ao público.

Diante do exposto, justifica-se a abertura de procedimento licitatório para a **contratação regular de serviços comuns e continuados de gerenciamento de TI**, garantindo:

- A continuidade das atividades institucionais do CRCES;
- A observância aos princípios da legalidade, eficiência e economicidade;
- A proteção de dados sensíveis, conforme previsto na LGPD;
- A segurança, estabilidade e evolução da infraestrutura tecnológica do Conselho

2.2 - PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

A contratação possui previsão no Plano de Contratações Anual do CRCES para o exercício 2026, e no Plano Diretor de Tecnologia da Informação.

2.3 - REQUISITOS DA CONTRATAÇÃO

		ITEM 1			
SUBITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

2.3.1 A Contratada deverá prestar **serviços gerenciados de Tecnologia da Informação** que abrangem o **suporte técnico avançado** (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a **gestão de incidentes e mudanças**. O escopo prevê a **gestão completa da infraestrutura de redes** (LAN, VLAN e WLAN), com o **fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa**, e a **gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais**. Será responsável também pelo **monitoramento contínuo da infraestrutura**, com identificação e mitigação proativa de riscos, pela **manutenção preventiva e corretiva** de todo o parque de TI, pela **gestão e monitoramento dos links de internet**, pela **gestão e manutenção da infraestrutura hiperconvergente** e do **banco de dados em SQL Server**. Além disso, inclui o **fornecimento, instalação e gestão de um Firewall de Próxima Geração** e a **implementação e gestão de solução de backup local e em nuvem**. Os serviços atenderão a única localidade do CRCES, até **60 estações de trabalho** (físicas ou virtuais), **5 servidores físicos** e **12 servidores virtuais**.

2.3.2 A empresa contratada deverá estar plenamente capacitada para **gerenciar toda a estrutura de TI híbrida do CRCES**. Esta estrutura é

complexa e inclui uma **infraestrutura hiperconvergente** (com armazenamento baseado em Software-defined Storage - SDS), uma **infraestrutura com acessos VDI (Virtual Desktop Infrastructure) máquinas virtuais** e uma **infraestrutura tradicional** (com desktops físicos e notebooks). A Contratada será responsável por assegurar a **gestão completa dos backups e restores** de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a **disponibilidade e integridade dos dados** em todas as plataformas.

2.4 CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS

2.4.1. SOLUÇÃO DE ACESSO VIA WI-FI.

2.4.1.1. Características da solução.

2.4.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

2.4.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

2.4.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

2.4.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

2.4.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

2.4.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

2.4.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.4.1.1.8. Site Survey Preliminar

Para a definição da quantidade de **equipamentos** necessários, conforme detalhado no item 2.4.1.1.2, o CRCES realizou um **levantamento de campo (site survey)** preliminar, cujos resultados são apresentados a seguir:

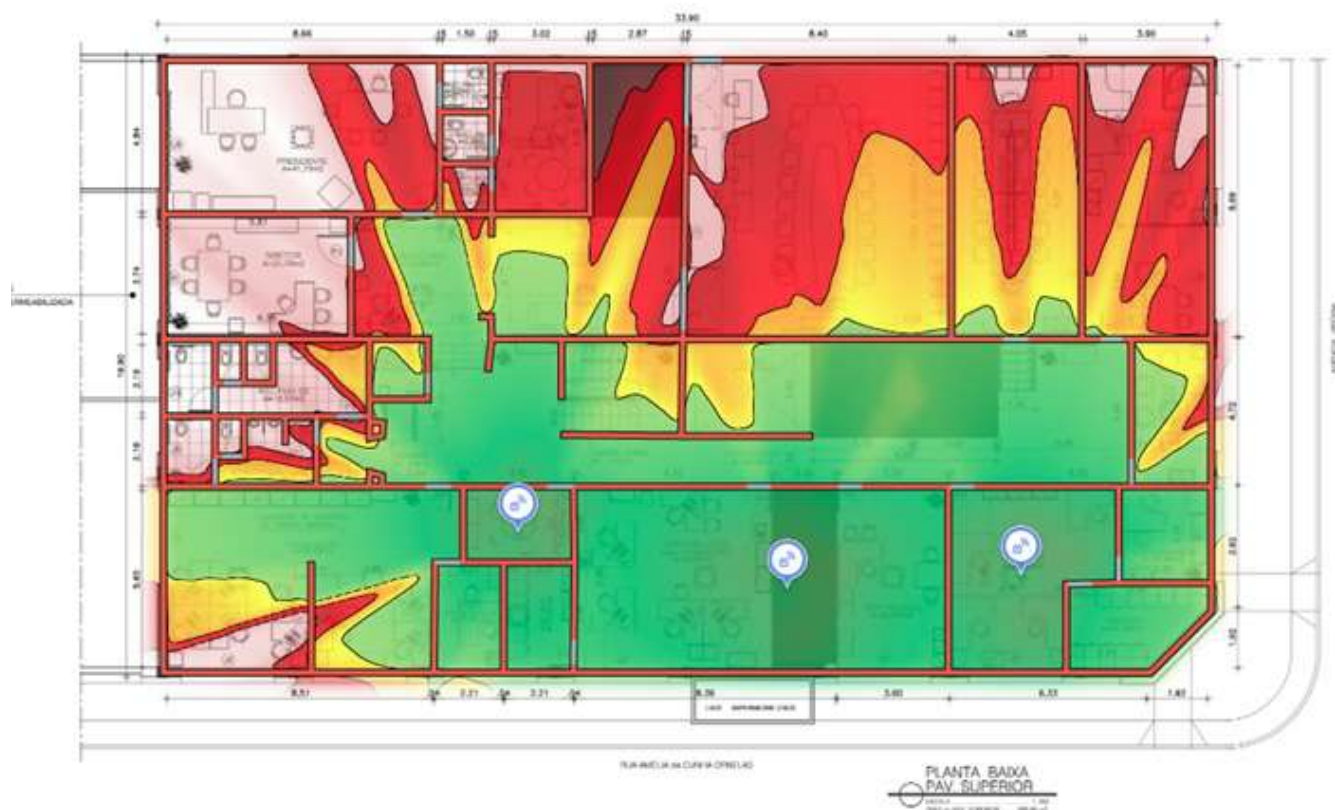
a) Pavimento térreo - 09 equipamentos





b) Pavimento superior - 09 equipamentos







2.5 CARACTERÍSTICAS DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.

2.5.1. Características dos pontos de acesso à internet via Wifi. (Equivalente ao seu antigo 1.2)

2.5.1.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

2.5.1.2. Deve ser compatível e gerenciado pelo ITENS "Firewall de Próxima Geração (NGFW) – Tipo 0x" deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

2.5.1.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

2.5.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

2.5.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

2.5.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

2.5.1.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

2.5.1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

2.5.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

2.5.1.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

2.5.1.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

2.5.1.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

2.5.1.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power

Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

2.5.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

2.5.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

2.5.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.5.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.5.1.20. Deve permitir operação em modo Mesh;

2.5.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

2.5.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

2.5.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

2.5.1.24. Deve suportar OFDMA;

2.5.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;

2.5.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

2.5.1.27. Deve suportar BSS Coloring;

2.5.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

2.5.1.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;

2.5.1.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);

2.5.1.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;

2.5.1.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;

2.5.1.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

2.5.1.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.5.1.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

2.5.1.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

2.5.1.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);

2.5.1.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

2.5.1.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

2.5.1.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

2.5.1.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.5.1.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.5.1.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.5.1.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.5.1.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.5.1.46. Deve implementar o padrão IEEE 802.11e;

2.5.1.47. Deve implementar o padrão IEEE 802.11h;

2.5.1.48. Deve implementar o padrão IEEE 802.3az;

2.5.1.49. Deve suportar ser gerenciado via SNMP;

2.5.1.50. Deve suportar consultas via REST API;

2.5.1.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

2.5.1.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;

2.5.1.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

2.5.1.54. Deve possuir indicadores luminosos (LED) para indicação de status;

2.5.1.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

2.5.1.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

2.5.1.57. Deve possuir certificado emitido pela Wi-Fi Alliance;

2.5.1.58. Deve estar homologado pela ANATEL na data de execução do pregão;

2.5.1.59. Deve ser licenciado para uso pelo período de duração da contratação.

2.5.1.60. Deve possuir garantia para uso pelo período de duração da contratação.

2.5.1.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

2.6. CARACTERÍSTICAS DO EQUIPAMENTO CONTROLADOR DE PONTOS DE ACESSO WIFI

2.6.1. Características do equipamento controlador de pontos de acesso Wifi (Equivalente ao seu antigo 1.3)

2.6.1.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

2.6.1.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

2.6.1.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

2.6.1.4. Deverá implementar os padrões IEEE 802.3af (PoE) e IEEE 802.3at (PoE+) com PoE budget de 370W em 24 portas;

2.6.1.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

2.6.1.6. Deve possuir 1 (uma) interface USB;

2.6.1.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);

2.6.1.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

2.6.1.9. Deve possuir tabela MAC com suporte a 32.000 endereços;

2.6.1.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

2.6.1.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

2.6.1.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (LACP);

2.6.1.13. Deve suportar a comutação de Jumbo Frames;

2.6.1.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

2.6.1.15. Deve implementar roteamento (camada 3) do modelo OSI entre as VLANs;

2.6.1.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

2.6.1.17. Deve implementar serviço de DHCP Relay;

2.6.1.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

2.6.1.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

2.6.1.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (RSTP) e IEEE 802.1s (MST). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

2.6.1.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

2.6.1.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

2.6.1.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

2.6.1.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

2.6.1.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

2.6.1.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

2.6.1.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

2.6.1.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

2.6.1.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

2.6.1.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

2.6.1.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

2.6.1.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

2.6.1.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

2.6.1.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

2.6.1.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

2.6.1.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

2.6.1.37. Deve suportar MAC Authentication Bypass (MAB);

2.6.1.38. Deve implementar RADIUS CoA (Change of Authorization);

2.6.1.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

2.6.1.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

2.6.1.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

2.6.1.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

2.6.1.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

2.6.1.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

2.6.1.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

2.6.1.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

2.6.1.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

2.6.1.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

2.6.1.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

2.6.1.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

2.6.1.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

2.6.1.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

- 2.6.1.53. Deve permitir ser gerenciado através de IPv6;
- 2.6.1.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 2.6.1.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 2.6.1.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 2.6.1.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 2.6.1.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 2.6.1.59. Deverá suportar ser configurado e monitorado através de REST API;
- 2.6.1.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 2.6.1.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 2.6.1.62. Deve suportar temperatura de operação de até 45º Celsius;
- 2.6.1.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 2.6.1.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 2.6.1.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 2.6.1.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 2.6.1.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 2.6.1.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

2.7 REQUISITOS DA INSTALAÇÃO DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.

- 2.7.1. Requisitos para instalação do item 1.2
- 2.7.2. Serviço de Implementação para rede WLAN
- 2.7.3. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura total, sendo observada a quantidade mínima estabelecida pela DTIC.
- 2.7.4. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;
- 2.7.5. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;
- 2.7.6. Requisitos gerais de Implantação
- 2.7.7. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.
- 2.7.8. Instalação física
- 2.7.9. Será realizada instalação física conforme a necessidade da contratante.
- 2.7.10. O ponto de acesso wifi deverá ser fixado no teto ou parede.
- 2.7.11. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

2.8 IMPLEMENTAÇÃO LÓGICA

- 2.8.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir
- 2.8.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.
- 2.8.3. Cadastro das subscrições dos APs na plataforma de gerência;
- 2.8.4. Endereçamento e segmentação das Redes WIRELESS;
- 2.8.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless);
- 2.8.6. Definição de políticas de bloqueio e permissão de acesso;
- 2.8.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 2.8.8. Configuração de Endereços/Interfaces de Gerência;
- 2.8.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 2.8.10. Parâmetros SNMP para monitoração/gerência remota;
- 2.8.11. Configuração de Syslog, quando aplicável;
- 2.8.12. Configuração de redes locais (VLANs);
- 2.8.13. Configuração de redes locais (SSIDs);
- 2.8.14. Configuração de sincronismo de hora NTP ou SNTP;
- 2.8.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 2.8.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 2.8.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 2.8.18. Configurações de grupos de ponto de acesso;
- 2.8.19. Configuração de algoritmo de criptografia a ser utilizado;
- 2.8.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 2.8.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 2.8.22. Configuração de segurança de rede;
- 2.8.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 2.8.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 2.8.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;

2.8.26. Emissão de relatórios de implantação contendo:

- 2.8.27. Mapas de rede,
- 2.8.28. Relação de equipamentos implantados,
- 2.8.29. Configurações feitas nos softwares;
- 2.8.30. Resultado dos testes realizados;

2.9 REQUISITOS PARA INSTALAÇÃO DO CONTROLADOR DE PONTOS DE ACESSO WIFI

2.9.1. Todo o processo de instalação será precedido de um estudo e entendimento de toda a infraestrutura em funcionamento hoje no ambiente englobando sua topologia, todas as configurações em uso (endereçamentos IP, VLANs, rotas, QoS, ACL's, etc),

2.9.2. Para a implementação da solução bem como acompanhamento do projeto proposto, a licitante deverá apresentar profissionais certificados, níveis avançados de conhecimento nas tecnologias ofertadas e necessárias para implantação da solução proposta.

2.9.3. O serviço de instalação, configuração da rede precederá de um cronograma de projeto para implementação das ações abaixo descritas, a ser elaborado de comum acordo.

2.9.4. Todo serviço deverá ser realizado por profissional do fabricante ou certificado por ele para execução dos serviços, para isso deverá ser apresentado junto com a proposta o certificado do profissional que irá executar os serviços de implantação

2.9.5. Planejamento e Projeto para Instalação da Solução

2.9.6. Levantamento e análise da configuração atual da rede;

2.9.7. Elaboração de Projeto de Rede detalhado em conjunto com a equipe de tecnologia da informação, incluindo os itens de configuração a seguir:

2.9.8. Endereçamento e segmentação das Redes LAN e WAN;

2.9.9. Roteamento estativo e dinâmico utilizando protocolos RIPv2 e OSPFv2, se aplicável;

2.9.10. Qualidade de Serviço (QoS): regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede;

2.9.11. Segurança:

2.9.12. Dos ativos: protocolos de comunicação segura, autenticação para acesso e proteção contra ataques;

2.9.13. Da rede: controles a serem implementados para restringir o acesso à rede e reduzir a exposição dos servidores e estações de trabalho;

2.9.14. Instalação da Solução

2.9.15. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;

2.9.16. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

2.9.17. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;

2.9.18. Configuração de Endereços/Interfaces de Gerência;

2.9.19. Endereçamento IP;

2.9.20. Telnet, se necessário;

2.9.21. Secure Shell (SSH), se necessário;

2.9.22. Web (HTTP), se necessário;

2.9.23. Restrições (Filtros/ACLs) de Acesso;

2.9.24. Autenticação;

2.9.25. Parâmetros SNMP para monitoração/gerência remota;

2.9.26. Configuração de redes locais (VLANs);

2.9.27. Configuração de sincronismo de hora NTP ou SNTP;

2.9.28. Configuração do protocolo Rapid Spanning Tree (RSTP);

2.9.29. Configuração de BPDU GUARD;

2.9.30. Configuração de Root Spanning Tree;

2.9.31. Interfaces de roteamento IP;

2.9.32. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;

2.9.33. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;

2.9.34. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.35. Otimização da Solução

2.9.36. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

2.9.37. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.38. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;

2.9.39. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto

2.9.40. Ativação de recursos para o controle de broadcast storms;

2.9.41. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.42. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.43. Controle de acesso a rede através do padrão IEEE 802.1x;

2.9.44. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;

2.9.45. Configuração de DHCP Snooping;

2.9.46. Configuração de DHCP Relay;

2.9.47. Configuração de interface confiável (trust Interface);

2.9.48. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.

2.9.49. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;

2.9.50. Criação e ativação de regras de acesso e perfis de acesso à rede;

2.9.51. Configuração de parâmetros de qualidade de serviço (QoS);

2.9.52. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;

2.9.53. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;

2.9.54. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;

2.9.55. Ativação e teste das ACLs nos equipamentos fornecidos;

2.9.56. Homologação

2.9.57. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.

2.9.58. Documentação em formato PDF contendo os itens a seguir:

2.9.59. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.

2.9.60. Arquivos de configuração dos ativos de rede;

2.9.61. Backup das configurações dos softwares utilizados;

2.9.62. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega;

2.10. Requisitos para instalação do cabeamento

- 2.10.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;
- 2.10.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;
- 2.10.3. Conectorização e crimpagem dos cabos em ambos os extremos;
- 2.10.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;
- 2.10.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;
- 2.10.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;
- 2.10.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;
- 2.10.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

2.11. Descrição do suporte continuado

- 2.11.1. A CONTRATADA deverá prestar assistência em horário comercial, das 07:30 às 16:30h na modalidade 8x5;
- 2.11.2. A CONTRATADA deverá providenciar a imediata reposição de equipamentos que estejam indisponíveis, seja por manutenção preventiva, seja por manutenção corretiva, avarias, acidentes ou paralisados por falhas provocadas por falta de suprimento, no prazo máximo de 24 (vinte e quatro) horas;

2.11.3. Da Manutenção Preventiva

A Contratada é a única e exclusiva responsável pela manutenção preventiva dos equipamentos objeto desta contratação; A manutenção deve obedecer às recomendações do fabricante de cada equipamento, porém, sem se limitar a elas e aos serviços abaixo descritos:

- 2.11.4. Providenciar revisão geral de todos os itens previstos de acordo com a recomendação do fabricante;
- 2.11.5. Verificar o estado geral de conservação dos equipamentos e providenciar substituição dos mesmos sempre que for necessário;
- 2.11.6. Efetuar as revisões periódicas, observando as recomendações do fabricante;
- 2.11.7. A Contratada deverá realizar as manutenções preventivas para garantir o pleno funcionamento dos equipamentos e a qualidade dos materiais produzidos.

2.11.8. Manutenção Corretiva

- 2.11.9. A manutenção corretiva deverá ocorrer sempre que a substituição do equipamento for necessária por quebra, assim como quando surgirem falhas;
- 2.11.10. A CONTRATADA deverá iniciar a manutenção corretiva em um prazo máximo de 4 (quatro) horas após a notificação por parte da CONTRATANTE, respeitando os horários definidos pela CONTRATANTE para essa tarefa;
- 2.11.11. A CONTRATADA deverá arcar com todos os custos decorrentes de avarias, exceto os decorrentes do mau uso do equipamento por parte do Contratante; Nesses casos, será de responsabilidade do Contratante arcar com os custos de reparo do equipamento;
- 2.11.12. A CONTRATADA deverá assumir integral e absoluta responsabilidade pelos equipamentos locados, desobrigando a CONTRATANTE de qualquer ônus, encargos, deveres e responsabilidade por defeitos, vícios aparentes ou ocultos, ou funcionamento insatisfatório dos aludidos bens e acidentes.

2.11.13. Serviço continuado

- 2.11.14. CONTRATADA deverá assumir a responsabilidade pelo gerenciamento da WLAN no que tange as seguintes ações:
- 2.11.15. Provisionamento e descoberta de dispositivos;
- 2.11.16. Prestar suporte técnico remoto e presencial;
- 2.11.17. Realizar atualizações de firmware e patches de segurança nos equipamentos;
- 2.11.18. Fazer a gestão de capacidade, espectro e canais da rede wireless;
- 2.11.19. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 2.11.20. Monitorar continuamente a saúde dos dispositivos
- 2.11.21. Monitorar perfil de usuário;
- 2.11.22. Monitorar Autenticação de usuários;
- 2.11.23. Proteção e implementação de WLAN usando os protocolos de segurança descritos no TR;
- 2.11.24. Entregar relatórios mensais com análise de disponibilidade, uso de canais, desempenho e incidentes;
- 2.11.25. Substituir equipamentos com defeito conforme cláusulas de SLA;
- 2.11.26. Corrigir falhas em conectores, cabos, patch panels e pontos RJ45 usados na solução;

2.12. ITEM - FIREWALL (SEDE)

- 2.12.1. Características da solução
 - 2.12.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
 - 2.12.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
 - 2.12.1.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
 - 2.12.1.4. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
 - 2.12.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução
 - 2.12.1.6. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço
 - 2.12.1.7. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.
 - 2.12.1.8. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

2.12.2. Requisitos técnicos dos equipamentos que compõe a solução

- 2.12.2.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.12.2.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;
- 2.12.2.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;
- 2.12.2.4. Deve Suportar, no mínimo, 65.000 (sessenta e cinco mil) Conexões de throughput VPN IPSec

- 2.12.2.4. Deve suportar, no mínimo, 0,5 (seis virgula cinco) Gbps de throughput VPN IPsec;
- 2.12.2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;
- 2.12.2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;
- 2.12.2.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;
- 2.12.2.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
- 2.12.2.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.
- 2.12.2.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;
- 2.12.2.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;
- 2.12.2.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;
- 2.12.2.13. Deve possuir porta console RJ-45;
- 2.12.2.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;
- 2.12.2.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
- 2.12.2.16. Deve possuir Fontes redundantes.
- 2.12.2.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.
- 2.12.2.18. Deve ser licenciado para uso pelo período de duração do contrato.
- 2.12.2.19. Deve possuir garantia para uso pelo período de duração do contrato.
- 2.12.3. Firewalls de próxima geração (NGFW).
- 2.12.3.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
- 2.12.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.12.3.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 2.12.3.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 2.12.3.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
- 2.12.3.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.
- 2.12.3.7. Funcionalidades de rede e firewall.**
- 2.12.3.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 2.12.3.7.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 2.12.3.7.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.12.3.7.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 2.12.3.7.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.12.3.7.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
- 2.12.3.7.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.12.3.7.8. Deverá suportar sFlow ou Netflow;
- 2.12.3.7.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 2.12.3.7.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 2.12.3.7.11. Deve suportar o protocolo padrão da indústria VXLAN;
- 2.12.3.7.12. Deve implementar o protocolo ECMP;
- 2.12.3.7.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 2.12.3.7.14. Enviar log para sistemas de monitoração externos;
- 2.12.3.7.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 2.12.3.7.16. Deve possuir mecanismos de proteção anti-spoofing;
- 2.12.3.7.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 2.12.3.7.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.12.3.7.19. Suportar OSPF graceful restart;
- 2.12.3.7.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.12.3.7.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 2.12.3.7.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 2.12.3.7.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 2.12.3.7.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 2.12.3.7.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 2.12.3.7.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 2.12.3.7.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 2.12.3.7.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 2.12.3.7.31. Deverá suportar controle por zonas de segurança;
- 2.12.3.7.32. Deverá suportar controles de políticas por porta e protocolo;
- 2.12.3.7.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 2.12.3.7.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 2.12.3.7.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 2.12.3.7.36. Controle, inspeção e descifração de SSL por política para tráfego de saída (Outbound).

2.12.3.7.36. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
2.12.3.7.37. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
2.12.3.7.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
2.12.3.7.39. Suporte a objetos e regras IPV6;
2.12.3.7.40. Suporte a objetos e regras multicast;
2.12.3.7.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

2.12.3.8. Funcionalidade de controle de aplicações.

2.12.3.8.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2.12.3.8.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
2.12.3.8.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
2.12.3.8.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
2.12.3.8.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
2.12.3.8.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
2.12.3.8.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
2.12.3.8.8. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
2.12.3.8.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
2.12.3.8.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
2.12.3.8.11. Atualizar a base de assinaturas de aplicações automaticamente;
2.12.3.8.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
2.12.3.8.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
2.12.3.8.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
2.12.3.8.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
2.12.3.8.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
2.12.3.8.17. Deve alertar o usuário quando uma aplicação for bloqueada;
2.12.3.8.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
2.12.3.8.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
2.12.3.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
2.12.3.8.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
2.12.3.8.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
2.12.3.8.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

2.12.3.9. Funcionalidade de prevenção de intrusão de ameaças.

2.12.3.9.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
2.12.3.9.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
2.12.3.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
2.12.3.9.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e "quarentenar" IP do atacante por um intervalo de tempo;
2.12.3.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
2.12.3.9.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
2.12.3.9.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
2.12.3.9.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
2.12.3.9.9. Deve permitir o bloqueio de vulnerabilidades;
2.12.3.9.10. Deve permitir o bloqueio de exploits conhecidos;
2.12.3.9.11. Deve incluir proteção contra-ataques de negação de serviços;
2.12.3.9.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
2.12.3.9.13. Detectar e bloquear a origem de portscans;
2.12.3.9.14. Bloquear ataques efetuados por worms conhecidos;
2.12.3.9.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
2.12.3.9.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
2.12.3.9.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

- 2.12.3.9.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.12.3.9.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.12.3.9.20. Identificar e bloquear comunicação com botnets;
- 2.12.3.9.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.12.3.9.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 2.12.3.9.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.12.3.9.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 2.12.3.9.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 2.12.3.9.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 2.12.3.9.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 2.12.3.9.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

2.12.3.10. Funcionalidade de filtro de conteúdo web e dns.

- 2.12.3.10.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.12.3.10.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 2.12.3.10.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 2.12.3.10.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 2.12.3.10.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.12.3.10.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 2.12.3.10.7. Possuir pelo menos 70 (setenta) categorias de URLs;
- 2.12.3.10.8. Deve possuir a função de exclusão de URLs do bloqueio;
- 2.12.3.10.9. Permitir a customização de página de bloqueio;
- 2.12.3.10.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 2.12.3.10.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 2.12.3.10.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 2.12.3.10.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

2.12.3.11. Funcionalidade de identificação de usuários.

- 2.12.3.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
- 2.12.3.11.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 2.12.3.11.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 2.12.3.11.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 2.12.3.11.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 2.12.3.11.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.12.3.11.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 2.12.3.11.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

2.12.3.12. Funcionalidade de filtro de dados .

- 2.12.3.12.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 2.12.3.12.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.12.3.13. Funcionalidade de geolocalização.

- 2.12.3.13.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 2.12.3.13.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.12.3.14. Funcionalidade de vpn.

- 2.12.3.14.1. Suportar VPN Site-to-Site e Cliente-To-Site;
- 2.12.3.14.2. Suportar IPSec VPN;
- 2.12.3.14.3. A VPN IPSEC deve suportar 3DES;
- 2.12.3.14.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 2.12.3.14.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

- 2.12.3.14.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.12.3.14.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.12.3.14.8. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 2.12.3.14.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.12.3.14.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPsec IPv6;
- 2.12.3.14.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.12.3.14.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 2.12.3.14.13. Atribuição de DNS nos clientes remotos de VPN;
- 2.12.3.14.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 2.12.3.14.15. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 2.12.3.14.16. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.12.3.14.17. Deverá manter uma conexão segura com o portal durante a sessão;
- 2.12.3.14.18. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

2.12.3.15. Funcionalidade de qos, traffic shaping e priorização de tráfego.

- 2.12.3.15.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- 2.12.3.15.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
- 2.12.3.15.3. Endereço de origem e Endereço de destino;
- 2.12.3.15.4. Usuário e grupo;
- 2.12.3.15.5. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 2.12.3.15.6. Por porta;
- 2.12.3.15.7. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 2.12.3.15.8. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
- 2.12.3.15.9. O QoS deve possibilitar a definição de fila de prioridade;
- 2.12.3.15.10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 2.12.3.15.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 2.12.3.15.12. Suportar modificação de valores DSCP para o Diffserv;
- 2.12.3.15.13. Suportar priorização de tráfego usando informação de ToS (Type of Service);
- 2.12.3.15.14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 2.12.3.15.15. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- 2.12.3.15.16. Deve possibilitar a definição de bandas distintas para download e upload;

2.12.3.16. Funcionalidade de balanceamento inteligente de links.

- 2.12.3.16.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 2.12.3.16.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
- 2.12.3.16.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 2.12.3.16.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 2.12.3.16.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 2.12.3.16.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 2.12.3.16.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
- 2.12.3.16.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 2.12.3.16.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 2.12.3.16.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
- 2.12.3.16.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 2.12.3.16.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 2.12.3.16.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 2.12.3.16.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 2.12.3.16.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 2.12.3.16.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 2.12.3.16.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

2.12.3.16.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

2.12.3.16.19. A solução deve possuir recurso para controlar e corrigir erros (FEC - Forward Error Correction) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

2.12.3.16.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

2.12.3.16.21. A solução deve suportar nativamente conectores com clouds públicas;

2.12.3.16.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

2.12.3.16.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

2.12.3.16.24. Deve implementar balanceamento de link por hash do IP de origem;

2.12.3.16.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

2.12.3.16.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

2.12.3.16.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

2.12.3.16.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

2.12.3.17. Funcionalidade de controlador de rede sem fio.

2.12.3.17.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

2.12.3.17.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

2.12.3.17.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

2.12.3.17.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

2.12.3.17.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

2.12.3.17.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

2.12.3.17.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

2.12.3.17.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de **túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

2.12.3.17.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPsec;

2.12.3.17.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.12.3.17.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.12.3.17.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

2.12.3.17.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

2.12.3.17.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.12.3.17.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

2.12.3.17.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

2.12.3.17.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

2.12.3.17.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como **Rogue APs**. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

2.12.3.17.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

2.12.3.17.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

2.12.3.17.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

2.12.3.17.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

2.12.3.17.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID

2.12.3.17.23. A solução deve permitir o agrupamento de pontos de acesso para que sejam distribuídas múltiplas subredes em um determinado sub, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

2.12.3.17.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

2.12.3.17.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

2.12.3.17.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

2.12.3.17.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.12.3.17.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.12.3.17.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.12.3.17.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

2.12.3.17.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

2.12.3.17.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

2.12.3.17.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.12.3.17.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

2.12.3.17.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

2.12.3.17.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

2.12.3.17.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;

2.12.3.17.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.12.3.17.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

2.12.3.17.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

2.12.3.17.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

2.12.3.17.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

2.12.3.17.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

2.12.3.17.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

2.12.3.17.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

2.12.3.17.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES)**;

2.12.3.17.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

2.12.3.17.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

2.12.3.17.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

2.12.3.17.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.12.3.17.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

2.12.3.17.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.12.3.17.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

2.12.3.17.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

2.12.3.17.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

2.12.3.17.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

2.12.3.17.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

2.12.3.17.58. A solução deve permitir a configuração do captive portal com endereço IPv6;

2.12.3.17.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

2.12.3.17.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

2.12.3.17.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

2.12.3.17.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

2.12.3.17.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

2.12.3.17.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

2.12.3.17.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será

disponibilizado;

2.12.3.17.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

2.12.3.17.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

2.12.3.17.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

2.12.3.17.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

2.12.3.17.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

2.12.3.17.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

2.12.3.17.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo **SNMP**;

2.12.3.17.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

2.12.3.17.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

2.12.3.17.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

2.12.3.17.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

2.12.3.17.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

2.12.3.17.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

2.12.3.17.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

2.12.3.17.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

2.12.3.17.81. A solução deve possuir ferramentas de diagnósticos e debug;

2.12.3.17.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

2.12.3.17.83. A solução deve suportar comunicação com elementos externos através de REST API;

2.12.3.17.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

2.12.3.18. Funcionalidade de controlador de rede cabeada.

2.12.3.18.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

2.12.3.18.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

2.12.3.18.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

2.12.3.18.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

2.12.3.18.5. Deve montar a topologia da rede de maneira automática;

2.12.3.18.6. Deve ser capaz de configurar os switches da rede;

2.12.3.18.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches

gerenciados;

2.12.3.18.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

2.12.3.18.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

2.12.3.18.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

2.12.3.18.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

2.12.3.18.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

2.12.3.18.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

2.12.3.18.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

2.12.3.18.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

2.12.3.18.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

2.12.3.18.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

2.12.3.18.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

2.12.3.18.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

2.12.3.18.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

2.12.3.18.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

2.12.3.18.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

2.12.3.18.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

2.12.3.18.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

2.13. Serviço de instalação firewall

2.13.1. Instalação Estrutura Física

2.13.1.1. Levantamento de toda estrutura física do ambiente;

2.13.1.2. Levantamento da estrutura Elétrica;

2.13.1.3. Verificação do espaço a ser instalado os equipamentos;

2.13.1.4. Abertura e conferência das caixas dos equipamentos;

2.13.1.5. Instalação do appliance físico;

2.13.1.6. Fixação do equipamento no RACK;

2.13.1.7. Conexão da fonte de alimentação elétrica em régua de tomada;

2.13.1.8. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;

2.13.1.9. Conexão das interfaces de rede com os switches;

2.13.2. Configuração do appliance físico:

2.13.2.1. Parametrização do Licenciamento;

- 2.13.2.2. Parametrização das interfaces de rede;
- 2.13.2.3. Atualização da última versão de Firmware;
- 2.13.2.4. Parametrização das regras de NAT;
- 2.13.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 2.13.2.6. Parametrização de Controle de Aplicação;
- 2.13.2.7. Parametrização de VPN (Virtual Private Network);
- 2.13.2.8. Parametrização IDS/IPS;
- 2.13.2.9. Parametrização DNS;
- 2.13.2.10. Parametrização de Gateway Antivírus;
- 2.13.2.11. Parametrização de Objetos de Endereço;
- 2.13.2.12. Parametrização de Grupo de Objetos;
- 2.13.2.13. Parametrização de Load Balancing;
- 2.13.2.14. Parametrização de SSO (Single Sign-on);
- 2.13.2.15. Parametrização de SNMP;
- 2.13.2.16. Parametrização de NTP;
- 2.13.2.17. Parametrização de PortGroups;
- 2.13.2.18. Parametrização de Zones;
- 2.13.2.19. Parametrização de Serviços;
- 2.13.2.20. Parametrização de Rotas;
- 2.13.2.21. Parametrização de DHCP

2.14. Serviços profissionais de suporte técnico na solução de firewall

- 2.14.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;
- 2.14.2. Efetuar toda rotina de backup das configurações semanalmente;
- 2.14.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

2.14.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

- 2.14.4.1. Atividades relativas à Solução de Segurança:
- 2.14.4.2. Criação das rotas para links.
- 2.14.4.3. Criação de NAT.
- 2.14.4.4. Liberação de portas.
- 2.14.4.5. Configuração do Filtro de Conteúdo.
- 2.14.4.6. Configuração do Controle de Aplicativos.
- 2.14.4.7. Configuração do Agente para autenticação LDAP.
- 2.14.4.8. Configuração para o Single Sign-On (SSO).
- 2.14.4.9. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 2.14.4.10. Configuração de VPN client to site.
- 2.14.4.11. Configuração de VPN site to site.
- 2.14.4.12. Criação de regras de Firewall.
- 2.14.4.13. Criação de regras de QoS.
- 2.14.4.14. Emitir relatório de segurança mensal por localidade.
- 2.14.4.15. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 2.14.4.16. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.
- 2.14.4.17. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

2.14.5. SLA dos serviços e atendimento

- 2.14.5.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 2.14.5.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 2.14.5.3. Gerar relatórios de acesso e desempenho da solução de firewall.
- 2.14.5.4. Deverá possuir sistema de abertura de chamados pela internet.
- 2.14.5.5. Monitorar latência e uptime dos links configurados.
- 2.14.5.6. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 2.14.5.7. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 2.14.5.8. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 2.14.5.9. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade

1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma

	continua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

2.15. Níveis de Severidade

2.15.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

2.15.2. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (quatro) horas úteis após o registro do chamado.

2.15.2.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

2.15.2.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.3. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.3.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser on-site e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

2.15.3.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.4. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.4.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência.

2.15.4.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.5. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.5.1. A CONTRATADA terá, no máximo, 8 (oito) dias corridos para solucionar o chamado, após o seu registro.

2.15.5.2. Não poderá haver limites no quantitativo de abertura de chamados.

2.16 Qualificação Técnica

2.16.1. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

2.16.2. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

2.16.3. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

2.16.4. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas;

2.16.5. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan, sendo que os trechos da documentação que comprovem os respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização.

3. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

3.1. Definição do objeto

3.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (Físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, abrangendo ativos de rede,

firewall (SonicWall), nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

3.1.2. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21da Lei nº 14.133, de 2021.

3.1.3. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar.

3.1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

3.1.5. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

3.1.6. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

3.2. Características da solução

3.2.1. A execução do objeto seguirá a seguinte dinâmica:

3.2.2. Início da execução do objeto: 05 (cinco) dias úteis da emissão da ordem de serviço;

3.2.3. Descrição detalhada:

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		SOLUÇÃO DE ACESSO VIA WI-FI	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		FIREWALL (SEDE)	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		BACKUP CORPORATIVO	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

3.2.4. Contratada deve prestar os serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente.

3.2.5. A empresa deverá estar pronta para gerir toda a estrutura hiperconvergente, que conta atualmente com dois clusters gerenciados de forma separada (com armazenamento baseado em Software-defined storage -SDS), uma infraestrutura com base em acessos VDI, máquinas virtuais. A empresa contratada deve estar pronta para lidar com seus backups, restores, e qualquer problema, falha, atualização, instalação ou análise oriunda desta relação de ferramentas integradas.

3.3. Requisitos técnicos

3.3.1. Monitoramento e suporte técnico

3.3.2. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;

3.3.3. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:

3.3.4. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);

3.3.5. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;

3.3.6. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;

3.3.7. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

3.3.8. Manutenção, gestão de ativos e rede

3.3.9. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados no item 6.1.1, sem custo adicional;

3.3.10. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;

3.3.11. Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.

3.3.12. Executar a gestão técnica da infraestrutura de rede, abrangendo:

3.3.13. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;

3.3.14. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;

3.3.15. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;

3.3.16. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.

3.3.17. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

3.3.18. Serviços gerenciados

3.3.19. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;

3.3.20. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;

3.3.21. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;

3.3.22. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

3.3.23. Controle, inventário e chamados

3.3.24. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;

3.3.25. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

3.3.26. Logística e apoio à contratação

3.3.27. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;

3.3.28. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:

3.3.29. Elaboração de especificações técnicas;

3.3.30. Análise de propostas técnicas;

3.3.31. Apoio em processos licitatórios;

3.3.32. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

3.3.33. Atendimento presencial

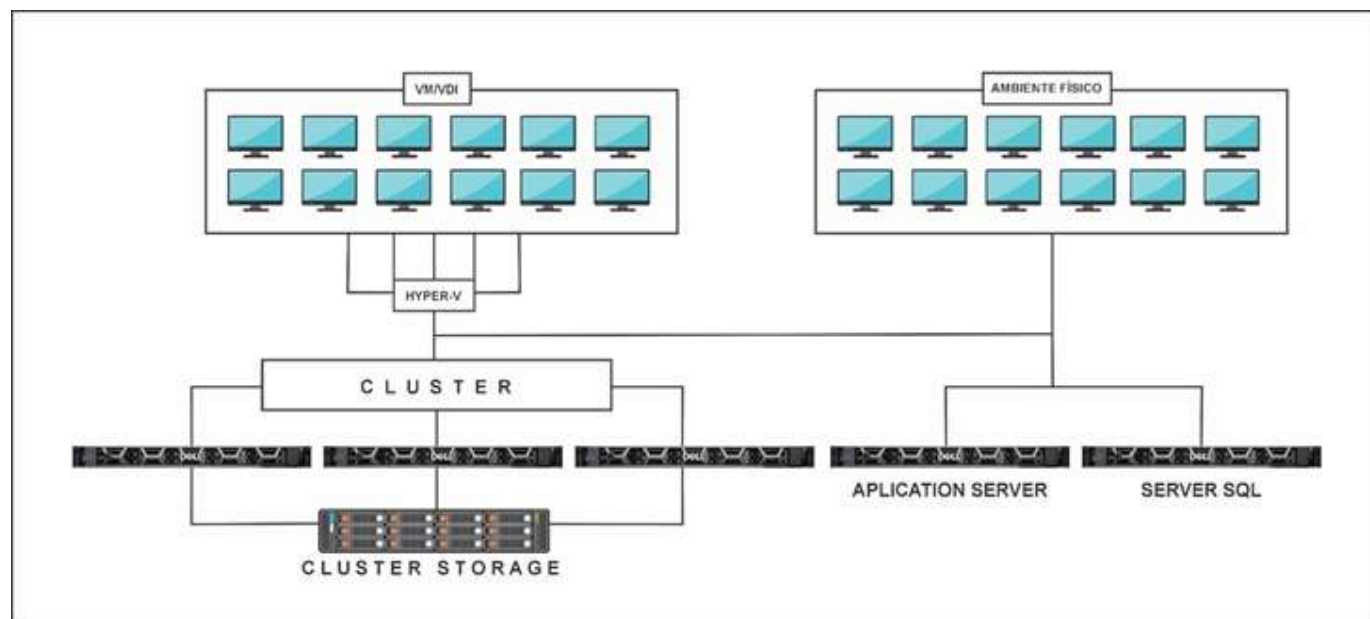
3.3.34. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 8 (oito) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

3.3.35. Parque de informática do CRCES:

TIPO	DESCRIÇÃO	QUANTIDADE
Equipamento de segurança	Firewall a ser contratado neste termo de referência	01
Pontos de acesso	Pontos de acesso a serem contratados neste termo de referência	A depender da solução contratada
Virtualizador	Hyper-V	05
Servidor Windows 2022 Server	Dell PowerEdge R640	02
Servidor Windows 2022 Server	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01
Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01

Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados - VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01

3.3.36. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



3.3.36. Manutenção Preventiva e Corretiva

3.3.36.1. Manutenção Preventiva

3.3.36.1.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

3.3.36.1.2. Tais atividades incluem, mas não se limitam a:

3.3.36.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

- 3.3.36.1.2.2. Limpeza técnica interna e externa;
- 3.3.36.1.2.3. Aferição e calibração de dispositivos, quando aplicável;
- 3.3.36.1.2.4. Atualização de firmwares, BIOS e softwares;
- 3.3.36.1.2.5. Verificação e otimização de configurações;
- 3.3.36.1.2.6. Avaliação do desempenho geral e análise de logs;
- 3.3.36.1.2.7. Testes de funcionalidade e conectividade.
- 3.3.36.1.3. Os equipamentos e ativos de tecnologia que deverão ser contemplados no plano de manutenção preventiva incluem:
 - 3.3.36.1.3.1. Servidores físicos;
 - 3.3.36.1.3.2. Servidores virtuais;
 - 3.3.36.1.3.3. Infraestrutura de rede (switches, cabeamento, racks, patch panels, etc.);
 - 3.3.36.1.3.4. Ativos de rede (roteadores, access points, controladoras, etc.);
 - 3.3.36.1.3.5. Estações de trabalho tipo desktop;
 - 3.3.36.1.3.6. Nobreaks e sistemas de energia ininterrupta;
 - 3.3.36.1.3.7. Terminais de desktop virtualizado (Thin Clients);
 - 3.3.36.1.3.8. Firewalls e appliances de segurança;
 - 3.3.36.1.3.9. Notebooks;
 - 3.3.36.1.3.10. Scanners (digitalizadores) de mesa e portáteis;
 - 3.3.36.1.3.11. Projetores multimídia;
 - 3.3.36.1.3.12. Monitores LCD/LED;
 - 3.3.36.1.3.13. Telefones IP e demais dispositivos de comunicação.
- 3.3.36.1.4. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.
- 3.3.36.1.5. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.
- 3.3.36.1.6. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.
- 3.3.36.1.7. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que solicitado.
- 3.3.36.2. Manutenção Corretiva
 - 3.3.36.2.1. Em caso de problema técnico, a contratada deverá providenciar laudo técnico e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.
 - 3.3.36.2.2. A CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.
 - 3.3.36.2.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.
 - 3.3.36.2.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.
 - 3.3.36.2.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.
 - 3.3.36.2.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 (cinco) dias úteis após o recebimento dos novos equipamentos/peças.
 - 3.3.36.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.
 - 3.3.36.2.8. Durante a execução do serviço externo, a empresa contratada deverá:
 - 3.3.36.2.8.1. Se responsabilizar pelo transporte dos equipamentos que serão retirados;
 - 3.3.36.2.8.2. Providenciar termo de responsabilidade de retirada;
 - 3.3.36.2.8.3. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.
 - 3.3.36.2.9. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;
 - 3.3.36.2.10. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;
 - 3.3.36.2.11. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;
 - 3.3.36.2.12. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;
 - 3.3.36.2.13. O recebimento definitivo não transfere a responsabilidade futura perante a validade do produto entregue.

- 3.3.36.2.13. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto a qualidade do produto entregue;
- 3.3.36.2.14. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.
- 3.3.37. SLA dos Serviços e Atendimento**
- 3.3.37.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 3.3.37.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 3.3.37.3. O ambiente de TI do CRCES deverá ser continuamente monitorado por ferramentas especializadas, com alertas automáticos e registro de falhas, a fim de garantir o funcionamento adequado e a disponibilidade dos recursos.
- 3.3.37.4. Deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos.
- 3.3.37.5. Deverá possuir sistema de abertura de chamados pela internet.
- 3.3.37.6. Monitorar latência e uptime dos links configurados.
- 3.3.37.7. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 3.3.37.7.1. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela (a ser fornecida ou referenciada no documento original).
- 3.3.37.7.2. Os níveis de atendimento técnico (N1, N2 e N3) deverão seguir o escopo descrito no item 3.3, com suporte remoto ilimitado e visitas técnicas presenciais duas vezes por semana (conforme cláusula 3.3.34).
- 3.3.37.7.3. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 3.3.37.8. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela (a ser fornecida ou referenciada no documento original).

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética (“cosméticos”), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

3.3.38 Níveis de Severidade

- **3.3.38.1.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.
- **3.3.38.2.** Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime **8x5 (on-site ou remota)**, com atendimento no local em até **4 (horas) horas úteis** após o registro do chamado.
 - **3.3.38.2.1.** Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a **8 (oito) horas úteis**, após o registro do chamado.
 - **3.3.38.2.2.** Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar **4 (quatro) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.3.** Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime **8x5 (remota ou on-site)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.3.1.** Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após **12 (doze) horas úteis**, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao **próximo dia útil**, após o registro do chamado.
 - **3.3.38.3.2.** Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.

- **3.3.38.4.** Para os chamados classificados como severidade 3 (tres), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.4.1.** A CONTRATADA terá, no máximo, **24 (Vinte e quatro) horas úteis**, após registro do chamado, para implantar uma solução definitiva ou de contingência.
 - **3.3.38.4.2.** Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias corridos** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.5.** Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
 - **3.3.38.5.1.** A CONTRATADA terá, no máximo, **8 dias corridos** para solucionar o chamado, após o seu registro.
 - **3.3.38.5.2.** Não poderá haver limites no quantitativo de abertura de chamados.

3.3.39 Qualificação Técnica

- **3.3.39.1.** A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se inviável:
- **3.3.39.2.** Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- **3.3.39.3.** Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.
- **3.3.39.4.** Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.
- **3.3.39.5.** Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.
- **3.3.39.6.** Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.
- **3.3.39.7.** Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.
- **3.3.39.8.** Certificação ITIL v3 ou superior;
- **3.3.39.9.** Certificação MCSA Windows Server 2012 ou superior;
- **3.3.39.10.** A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:
 - **3.3.39.10.1.** Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;
 - **3.3.39.10.2.** Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;
 - **3.3.39.10.3.** Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

4. BACKUP CORPORATIVO

4.1. Software de Backup

- **4.1.1.** Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- **4.1.2.** Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.
- **4.1.3.** Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- **4.1.4.** Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.
- **4.1.5.** Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.
- **4.1.6.** Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- **4.1.7.** Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.
- **4.1.8.** Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.
- **4.1.9.** Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.
- **4.1.10.** Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.
- **4.1.11.** Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.
- **4.1.12.** Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.

- 4.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações:** O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.
- 4.1.14. Backup Incremental e Diferencial:** Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.
- 4.1.15. Cópias de Backup Imutáveis:** Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.
- 4.1.16. Retenção Personalizável:** O software deve oferecer flexibilidade na configuração de políticas de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.
- 4.1.17. Arquivamento Inteligente:** Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.
- 4.1.18. Monitoramento e Alertas:** O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.
- 4.1.19. Dashboard Intuitivo:** Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.
- 4.1.20. Otimização de Recursos (IOPS e Throughput):** O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.
- 4.1.21. Restauração Granular:** Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.
- 4.1.22. Recuperação Bare-Metal:** Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.
- 4.1.23. Testes de Restauração Automática:** Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.
- 4.1.24. Integração Nativa com Provedores de Nuvem:** Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.
- 4.1.25. Economia de Largura de Banda:** Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.
- 4.1.26. Perfis de Acesso Personalizáveis:** O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.
- 4.1.27. Controle de Acessos Granular:** Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.
- 4.1.28. Suporte a LGPD e Outras Normas:** O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.
- 4.1.29. Auditorias e Relatórios:** Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.
- 4.1.30. Automatização de trabalhos de Backup:** Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.
- 4.1.31. Integração com Ferramentas de Orquestração:** Suporte para integração com ferramentas de orquestração e automação (ex: scripts PowerShell, APIs).
- 4.1.32. Cobertura Completa:** O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.
- 4.1.33. Recuperação Granular:** Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.
- 4.1.34. Agendamento e Automação:** A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

4.2. Appliance de Backup Local

- 4.2.1.** A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.
- 4.2.2.** Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.
- 4.2.3.** Será responsável por configurar o sistema de armazenamento local do equipamento, devendo:
- 4.2.3.1.** Criar e configurar o arranjo de discos em RAID 5;
- 4.2.3.2.** Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);
- 4.2.3.3.** Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas
- 4.2.4.** Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.
- 4.2.5.** Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:
- 4.2.5.1.** Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;
- 4.2.5.2.** Gerar e manter registros e relatórios de status dos backups locais e remotos;
- 4.2.5.3.** Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES.

4.2.5.5. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

4.2.6. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:

4.2.6.1. Acompanhamento da integridade dos discos e volumes lógicos;

4.2.6.2. Monitoramento do uso de espaço em disco e alertas proativos;

4.2.6.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

4.2.7. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:

4.2.7.1. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;

4.2.7.2. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).

4.2.8. deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:

4.2.8.1. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;

4.2.8.2. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;

4.2.8.3. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;

4.2.8.4. Ajustar as políticas de backup e monitoramento para o novo ambiente.

4.2.9. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

4.3. Armazenamento de backup em nuvem

4.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.

4.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.

4.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.

4.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.

4.3.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.

4.3.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.

4.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.

4.3.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).

4.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.

4.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.

4.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.

4.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.

4.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.

4.3.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.

4.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.

4.3.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.

4.3.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.

4.3.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).

4.3.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.

4.3.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e possíveis falhas.

4.3.23. Ferramentas de monitoramento nativas devem estar integradas.

4.3.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

4.4. SLA dos serviços e atendimento

- 4.4.1.** Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 4.4.2.** Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 4.4.3.** deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime e falhas críticas.
- 4.4.4.** Deverá possuir sistema de abertura de chamados pela internet.
- 4.4.5.** A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 4.4.6.** O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 4.4.7.** Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 4.4.8.** Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela , a seguir:

Níveis de Severidade	
1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.

3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup..
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

4.4.9. Níveis de Severidade

- 4.4.10.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.
- 4.4.11.** Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.
- 4.4.11.1.** Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.
- 4.4.11.2.** Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.
- 4.4.12.** Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.
- 4.4.12.1.** Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.
- 4.4.12.2.** Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.
- 4.4.13.** Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.
- 4.4.13.1.** A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência
- 4.4.13.2.** Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.
- 4.4.14.** Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.
- 4.4.14.1.** A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.
- 4.4.14.2.** Não poderá haver limites no quantitativo de abertura de chamados.

4.3.3.17. Certificações

Será necessário solicitar algumas certificações, com isso o CRCES está garantindo que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade, alinhado com as melhores práticas do mercado e com as recomendações de segurança de órgãos como o NIST e o CIS.

Abaixo, vamos citar cada uma delas, ampliando as justificativas:

a) Certificação Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 (no mínimo)

Domínio do Sistema Operacional: A certificação MCSA garante que o profissional possui um conhecimento profundo do Windows Server 2012,

que é a base do nosso ambiente corporativo hiperconvergente. Isso inclui domínio em instalação, configuração, administração e troubleshooting do sistema operacional, além de serviços como Active Directory, DNS, DHCP e outros.

Integração com Outros Serviços: O Windows Server é integrado a outros serviços da Microsoft, como Exchange, SharePoint e SQL Server. Um profissional com a certificação MCSA terá mais facilidade em integrar e gerenciar esses serviços em um ambiente unificado.

Padrão de Qualidade e Alinhamento com Boas Práticas: A certificação MCSA é reconhecida mundialmente como um padrão de qualidade para profissionais de infraestrutura. Ela demonstra que o profissional possui as habilidades necessárias para lidar com as complexidades de um ambiente como o nosso, que possui dois clusters e funciona no modelo de hiperconvergência, além de estar alinhado com as melhores práticas do mercado.

b) Certificação para Instalação e Configuração de Switches DELL ou similar

Infraestrutura de Rede e Otimização: Switches são equipamentos essenciais para a interconexão de dispositivos em uma rede. A certificação garante que o profissional possui conhecimento sobre os princípios de funcionamento de switches, além de saber como configurá-los para atender às necessidades específicas da rede do CRCES, que utiliza switches complexos de alta tecnologia (tanto o core quanto o de agregação da hiperconvergência). Isso permite otimizar o desempenho da rede, reduzindo a latência e aumentando a disponibilidade.

Escalabilidade e Flexibilidade: À medida que a rede cresce, é necessário adicionar novos switches. Um profissional certificado terá as habilidades necessárias para integrar novos switches à rede existente, garantindo a escalabilidade da infraestrutura e a flexibilidade para atender às futuras demandas do CRCES.

Alinhamento com as Melhores Práticas: A certificação garante que o profissional está familiarizado com as melhores práticas de configuração e gerenciamento de redes, o que contribui para a estabilidade e a segurança da infraestrutura.

As certificações solicitadas demonstram que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade para o CRCES. Elas garantem que os profissionais terão a capacidade de:

Gerenciar e manter a infraestrutura de TI de forma eficiente, segura e alinhada com as melhores práticas do mercado.

Resolver problemas de forma rápida e eficaz, minimizando o tempo de inatividade do sistema.

Implementar novas tecnologias de forma adequada e segura.

Acompanhar as melhores práticas do mercado e as recomendações de segurança de órgãos como o NIST e o CIS.

4.3.3.17.1. Justificativa

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada para gerar todos esses serviços de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

a) Assegurar a contratação da empresa mais qualificada e experiente para o serviço.

b) Definir claramente as expectativas e responsabilidades de ambas as partes.

c) Permitir a avaliação objetiva das propostas e a escolha da melhor solução.

d) Facilitar o acompanhamento e a fiscalização do contrato.

e) Mitigar riscos e garantir o sucesso da contratação.

f) Atender aos princípios da Lei 14.133 e da Administração Pública.

Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:

a) Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.

b) Aumento de custos com retrabalho, correções e possíveis perdas.

c) Dificuldades na comunicação e na resolução de conflitos.

d) Dificuldades na fiscalização do contrato e na cobrança de resultados.

e) Riscos de inadimplência e de litígios.

A contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.

4.3.3.18. Softwares que deverão ser disponibilizados

As ferramentas listadas abaixo (monitoramento e de abertura de chamados) deverão ser disponibilizadas e totalmente configuradas pela CONTRATADA sem custo adicional para o CRCES, e deverão apresentar as seguintes especificações (mínimas):

4.3.3.18.1. Ferramenta de monitoramento.

Monitoramento de Rede: Roteadores, switches, impressoras, etc., utilizando protocolos como SNMP (v1/v2c/v3), ICMP (ping) e verificações de portas TCP/UDP.

Monitoramento de Servidores: Desempenho de CPU, uso de memória, espaço em disco, tráfego de rede, processos, serviços e logs.

Monitoramento de Aplicações e Serviços: Bancos de dados (MySQL, PostgreSQL, Oracle, etc.), servidores web (Apache, Nginx, IIS), Java applications (JMX), serviços específicos e outros.

Monitoramento de Virtualização: Serviços em nuvem, contêineres, máquinas virtuais.

Monitoramento Web (Web Scenarios): Simula a navegação de usuários em aplicações web, verificando a disponibilidade, o tempo de resposta e o conteúdo das páginas.

Monitoramento de Dispositivos IoT e Sensores: Coleta dados de uma variedade de sensores e dispositivos IoT.

Monitoramento de Logs e Eventos: Analisa arquivos de log em busca de padrões, erros, avisos ou atividades suspeitas.

Extensibilidade: Permitir a coleta de dados qualquer fonte através de scripts externos personalizados, APIs e extensões.

Limiares Flexíveis: Definição de condições personalizadas para identificar problemas (triggers).

Previsão de Tendências e Machine Learning: Funções preditivas que permitem prever quando um limiar será atingido, possibilitando ações proativas antes que um problema ocorra.

Níveis de Severidade: Classificação dos problemas por níveis de severidade (informação, aviso, médio, alto, desastre), facilitando a priorização.

Análise de Causa Raiz: Ajuda a identificar a causa subjacente dos problemas.

Canais de Notificação Diversos: Envio de alertas por e-mail, SMS, aplicativos de mensagens (Telegram, Slack, etc.), webhooks e scripts personalizados.

Escalonamento de Alertas: Configuração de fluxos de escalonamento para garantir que os alertas cheguem aos destinatários corretos em diferentes etapas.

Ações Automáticas (Auto-remediação): Possibilidade de executar comandos remotos automaticamente em resposta a um problema (ex: reiniciar um serviço, executar um script de correção).

Notificações Customizáveis: Mensagens de alerta personalizadas com informações relevantes sobre o problema.

Dashboards Personalizáveis: Criação de painéis de controle interativos com widgets para exibir métricas em tempo real, status de hosts, problemas, mapas de rede, gráficos e muito mais.

Gráficos Flexíveis: Geração de gráficos detalhados para visualizar dados históricos e tendências, com opções de personalização de tempo e exibição.

Mapas de Rede (Network Maps): Criação de representações visuais da infraestrutura, mostrando o status dos dispositivos e as interconexões.

Relatórios: Geração de relatórios de disponibilidade, desempenho e outros dados relevantes.

Visão de Negócio (SLA/KPI): Possibilidade de monitorar o desempenho dos serviços de TI em relação aos Acordos de Nível de Serviço (SLAs) e Indicadores Chave de Desempenho (KPIs).

Descoberta Automática de Rede (Network Discovery): Detecta automaticamente novos dispositivos na rede, facilitando a configuração inicial.

Auto-registro de Agentes (Agent Autoregistration): Permite que os agentes Zabbix se registrem automaticamente no servidor Zabbix, simplificando a implantação em grande escala.

Descoberta de Baixo Nível (Low-Level Discovery - LLD): Descobre automaticamente componentes de um host (ex: interfaces de rede, sistemas de arquivos, CPUs, partições de disco) e cria itens de monitoramento, triggers e gráficos para eles.

Modelos (Templates): Reutilização de configurações de monitoramento para diferentes tipos de hosts, agilizando a implantação e padronizando o monitoramento.

Sistema de Permissões: Controle granular de acesso baseado em funções e grupos de usuários.

Autenticação: Suporte a diferentes métodos de autenticação (interna, LDAP, SAML).

criptografia: Criptografia de todo o tráfego de monitoramento para garantir a segurança dos dados.

Alta Disponibilidade: Monitoramento contínuo.

4.3.3.18.2. Ferramenta de abertura e gestão de chamados de T.I

Abertura de chamados por e-mail: Integração com e-mail para que os chamados sejam criados automaticamente a partir de mensagens enviadas para um endereço específico.

Categorização e Priorização Automática: Possibilidade de pré-definir categorias (ex: "Problema de Software", "Solicitação de Hardware", "Acesso"), subcategorias e níveis de prioridade (ex: "Baixa", "Média", "Alta", "Crítica") com base no tipo de solicitação ou no usuário.

Anexos: Capacidade de anexar arquivos (screenshots, logs, documentos) para fornecer mais contexto ao chamado.

Atribuição Automática e Manual: Atribuição de chamados a agentes ou equipes com base em regras predefinidas (categoria, prioridade, departamento do usuário) ou atribuição manual pelos gerentes.

Filas de Atendimento: Organização dos chamados em filas específicas para cada equipe ou tipo de serviço.

Fluxos de Trabalho (Workflows): Definição de etapas e ações automatizadas para o ciclo de vida de um chamado (ex: Aberto -> Em Andamento -> Aguardando Usuário -> Resolvido -> Fechado).

Notificações Automáticas: Envio de e-mails ou notificações push para o usuário e para os agentes sobre o status do chamado, novas mensagens, resolução, etc.

Colaboração em Equipe: Permite que múltiplos agentes trabalhem em um mesmo chamado, com compartilhamento de informações e anotações.

Macros/Respostas Predefinidas: Modelos de respostas para perguntas frequentes, agilizando o atendimento.

Artigos e FAQs: Repositório central de artigos de solução de problemas, FAQs (perguntas frequentes), guias e procedimentos.

Busca Inteligente: Ferramenta de busca robusta que permite aos usuários e agentes encontrar informações relevantes rapidamente.

Sugestão de Soluções: Apresentar artigos da base de conhecimento aos usuários enquanto eles digitam seu problema no portal self-service, incentivando a auto-resolução.

Dashboards e Métricas: Visualização em tempo real de KPIs (Key Performance Indicators) como número de chamados abertos, chamados resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

Relatórios Customizáveis: Geração de relatórios sobre desempenho da equipe, tipos de chamados mais comuns, cumprimento de SLAs, tendências, etc.

Integração com a ferramenta de Monitoramento: Integração com a ferramenta de monitoramento proposto pela CONTRATADA, para que alertas de monitoramento possam gerar chamados automaticamente.

Controle de Acesso Baseado em Funções: Definição de permissões diferentes para usuários, agentes e administradores.

Acessibilidade: Interface amigável e acessível em diferentes dispositivos (desktop, mobile).

SLA (Service Level Agreement) Management:

Definição de SLAs para diferentes tipos de chamados, especificando tempo de resposta e tempo de resolução esperados.

Monitoramento automático do cumprimento dos SLAs, com alertas e escalonamentos caso os prazos estejam sendo excedidos.

Escalonamento automático para gerentes ou equipes superiores quando os SLAs estão em risco.

Histórico Completo do Chamado: Registro detalhado de todas as interações, atualizações, comentários e mudanças de status em um chamado.

Pesquisa Avançada: Facilidade para buscar chamados por ID, usuário, categoria, palavras-chave, etc.

4.3.3.19. Serviços externos que deverão ser acompanhados pela contratada

A CONTRATADA será um ponto focal e estratégico para o CRCES, atuando como o principal **elo de coordenação e intermediação** entre nossa instituição e as demais prestadoras de serviços de TI. Dada a complexidade e a interdependência de nossas operações tecnológicas, a **intervenção e o acompanhamento proativo** da CONTRATADA serão cruciais para garantir a fluidez e a eficácia de todas as interações e projetos. Atualmente, gerenciamos diversos contratos com terceiros, e essa carteira de fornecedores poderá se expandir conforme nossas necessidades evoluírem. Abaixo vamos listar alguns dos contratos:

- Serviço de fornecimento de software de gestão integrada (SpiderWare);
- Serviço de hospedagem do website e webservice do CRCES;
- Serviço de fornecimento de link de internet;
- Serviço de fornecimento de e-mail corporativo;
- Serviço de fornecimento de link SIP Trunk;
- Serviço de fornecimento de validador de assinaturas digitais;
- Serviço de fornecimento de atendente virtual por whatsapp;
- Serviço de outsourcing de impressão;
- Serviço de fornecimento de ePABX;

5. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE DÃO SUPORTE;

5.1 A estimativa de quantidade foi baseada na estrutura de tecnologia atual do CRCES, conforme descrito ao longo deste documento.

6. LEVANTAMENTO DE MERCADO, ANÁLISE DAS ALTERNATIVAS POSSÍVEIS E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO T I SOLUÇÃO A CONTRATAR;

6.1 O levantamento de mercado para contratação de empresa que preste serviço de gerenciamento de T.I e um processo que requer atenção, cuidado e critério, pois envolve a confiança e a parceria entre o contratante e o contratado.

6.2 Atualmente, o CRCES enfrenta um cenário desafiador na gestão de T.I, com apenas um funcionário dedicado a essa área. Esta escassez representa um risco significativo para a continuidade dos serviços e para a qualidade do atendimento oferecido aos usuários.

6.3 Ademais, o CRCES se depara com desafios crescentes, como a necessidade premente de adaptação às normas de governança, a demanda por inovação e modernização tecnológica, bem como a crescente complexidade dos processos e projetos de T.I.

6.4 Em um ambiente em constante evolução tecnológica, é essencial que o CRCES esteja alinhado com as mais recentes tendências e práticas em T.I. A falta de recursos e expertise interna dificulta a implementação de soluções inovadoras que possam impulsionar a eficiência e a eficácia das operações.

6.5 O serviço de gerenciamento de T.I são considerados serviços comuns, pois se enquadram na definição de atividades que podem ser prestadas por qualquer pessoa jurídica, sem exigência de qualificação específica ou exclusividade.

6.6 Uma vez que há diversas empresas que oferecem este serviço, optamos por consultar empresas que já têm experiência com a infraestrutura tecnológica do CRCES, o que nos permite obter uma pesquisa mais adequada à realidade e à necessidade do suporte e serviço que solicitamos no processo, com isso, alcançamos a estimativa descrita abaixo:

	VALOR ITEM I
Mensal	R\$40.000,00
Anual	R\$480.000,00

6.7 Analisando os orçamentos apresentados, o valor mensal para esta contratação ficou estimado em R\$ 40.000,00 (quarenta mil reais), sendo que o valor total para os 12 (doze) meses resulta no valor de R\$480.000,00 (quatrocentos e oitenta mil reais) para os serviços gerenciados em Tecnologia da Informação.

CC-0/2025 - Comissão Permanente de Contabilidade da Prefeitura Santa Helena - 4478-0/2025 - Termo de responsabilidade de entrega de prestação de serviços

6.9 Além disso, o Conselho Regional de Contabilidade do Espírito Santo, como órgão público, tem a responsabilidade de zelar pelo uso eficiente dos recursos financeiros. Portanto, a busca pelo menor preço em processos de contratação é uma prática comum para garantir a economicidade e maximizar o retorno sobre o investimento público.

6.10 Outro aspecto relevante é a transparência e a simplificação do processo de licitação proporcionadas pelo critério de "menor preço". Por ser um critério objetivo de verificação, ele facilita a análise das propostas pelos licitantes e pelos responsáveis pela fiscalização, promovendo assim a lisura e a competitividade do certame.

6.10 Por fim, considerando que os **Serviços gerenciados em Tecnologia da Informação** são essenciais para garantir a saúde e a segurança dos ocupantes das instalações do Conselho Regional de Contabilidade, a escolha do critério de "menor preço" permite contar com uma infraestrutura de tecnologia da informação (T.I) eficiente, segura e atualizada, que garanta o bom funcionamento dos sistemas internos e externos, a comunicação com os diversos públicos e a proteção dos dados sensíveis.

6.11 Dessa forma, o uso do critério de "menor preço" no processo de licitação para a contratação de serviços **Tecnologia da Informação** completa é uma escolha justificada e alinhada aos princípios da administração pública, visando garantir a eficiência, a transparência e o melhor aproveitamento dos recursos disponíveis.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Conforme documentos acostados aos autos, o valor estimado da contratação mensal é de R\$40.000,00 (quarenta mil reais) perfazendo o valor total de R\$480.000,00 (quatrocentos e oitenta mil reais).

Para fins de estimativa da presente contratação, procedeu-se à pesquisa direta com fornecedores, por meio de solicitação de proposta de preço por e-mail, cujo valor médio é apresentado acima.

A pesquisa está em conformidade com o art. 6º da Instrução Normativa SEGES/ME n.º 65/2021, realizamos a média dos orçamentos.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, INCLUSIVE DAS EXIGÊNCIAS RELACIONADAS À MANUTENÇÃO E À ASSISTÊNCIA TÉCNICA, QUANDO FOR O CASO;

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

Na descrição da solução, já estão incluídos todos os procedimentos, equipamentos, instalação e manutenções corretivas para a perfeita execução dos serviços.

9. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO;

A não viabilidade de parcelamento da solução se fundamenta na natureza integrada do objeto, que demanda uma abordagem unificada para garantir eficiência e consistência. Optar por consolidar os serviços em um único item considerou a coesão dos elementos a serem licitados e a sequência lógica de sua execução.

Adicionalmente, a fragmentação deste processo acarretaria à Administração um risco significativo, pois diferentes empresas, embora possam operar no mesmo setor, apresentam disparidades estruturais, logísticas e econômico-financeiras. Tal divisão resultaria em capacidades discrepantes de prestação de serviço, comprometendo a supervisão e expondo a execução dos contratos a possíveis desvios dos padrões estabelecidos.

Portanto, a decisão de não parcelar a contratação busca assegurar a coerência e a qualidade na entrega dos serviços, minimizando potenciais incongruências e garantindo a conformidade na execução do objeto.

10. RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS;

Pretende-se com a presente contratação, os resultados abaixo descritos:

- Aumentar a eficiência e a segurança dos sistemas de informação do CRCES, reduzindo os riscos de falhas, perdas ou vazamentos de dados.
- Garantir a continuidade das atividades do CRCES em caso de eventuais problemas técnicos, desastres naturais ou ataques cibernéticos, por meio de um plano de recuperação de desastres baseado em backup em nuvem.
- Otimizar os custos e os recursos do CRCES, evitando gastos desnecessários com infraestrutura, manutenção e atualização de equipamentos e softwares.
- Melhorar o atendimento e a satisfação dos profissionais da contabilidade e da sociedade em geral, oferecendo serviços de qualidade, rapidez e confiabilidade.

11. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Para a execução do objeto deste estudo, não há necessidade de nenhuma adequação do ambiente do órgão.

12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES;

Para o objeto deste estudo, não são necessárias contratações correlatas ou interdependentes.

13. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, QUANDO APLICÁVEL;

Não se aplica a esta contratação.

14. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA.

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada em gerenciamento de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a. Assegurar a contratação da empresa mais qualificada e experiente para o serviço.
- b. Definir claramente as expectativas e responsabilidades de ambas as partes.
- c. Permitir a avaliação objetiva das propostas e a escolha da melhor solução.
- d. Facilitar o acompanhamento e a fiscalização do contrato.
- e. Mitigar riscos e garantir o sucesso da contratação.
- f. Atender aos princípios da Lei 14.133 e da Administração Pública.
- g. Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:
 - h. Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.
 - i. Aumento de custos com retrabalho, correções e possíveis perdas.
 - j. Dificuldades na comunicação e na resolução de conflitos.
 - k. Dificuldades na fiscalização do contrato e na cobrança de resultados.
 - l. Riscos de inadimplência e de litígios.
- m. Em suma, a contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.
- n. Investir em um Termo de Referência bem elaborado é um investimento na segurança, confiabilidade e no sucesso da gestão da TI do CRCES.
- o. Além disso, essa medida promove transparência e integridade, uma vez que impede o envolvimento de terceiras partes que possam diluir a responsabilidade direta da contratada. A restrição à exploração industrial visa, ainda, assegurar que o objeto seja destinado exclusivamente ao cumprimento das finalidades públicas, sem desvios para utilização comercial ou industrial que contrariem o interesse público.
- p. Para comprovação de capacidade, deve exigir-se que os licitantes apresentem atestados técnicos que demonstrem a execução dos serviços com infraestrutura própria e sem uso de exploração industrial, atendendo assim ao critério de "estrutura própria" e garantindo os altos padrões esperados.

Com base nas informações estabelecidas neste documento, nas justificativas apresentadas no Documento de Formalização da Demanda – DFD, a Equipe de Planejamento DECLARA a viabilidade da contratação de empresa especializada, Serviços de TI inclui a gestão de redes, ativos de rede, servidores, estações de trabalho, nobreaks e monitores. A empresa será responsável por suporte técnico remoto e presencial, manutenção preventiva e corretiva, e monitoramento de links de internet e infraestrutura hiperconvergente.

15. Normativos que disciplinam o serviço a ser contratado:

[Lei nº 14.133](#), de 1º de abril de 2021 - Lei de Licitações e Contratos Administrativos.

[Decreto nº 10.947](#), de 25 de janeiro de 2022 - Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

[Decreto nº 7.174](#), de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

[Instrução Normativa SGD/MGI nº 6](#) de 29 de março de 2023 - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

[Instrução Normativa SGD/ME nº 94](#) de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

[Instrução Normativa SLTI nº 01](#), de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

16. Do Acesso às Informações contidas nos presentes Estudos Preliminares:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que:

☒

As informações contidas nos presentes Estudos Preliminares **DEVERÃO ESTAR DISPONÍVEIS** para qualquer interessado, pois não se caracterizam como sigilosas.

☐

As informações contidas nos presentes Estudos Preliminares **ASSUMEM CARÁTER SIGILOSOS**. Nos termos do Art. 23 da Lei nº 12.527/2011, e, portanto, deverão ter acesso restrito.

17. Equipe de Planejamento:

São responsáveis pela elaboração do presente documento que materializa os Estudos Preliminares da presente contratação os seguintes servidores:

Wekson José Barbieri Mariano

Matrícula 87

Membro da Equipe de Planejamento

Elaine Leopoldino Ferreira

Matrícula 198

Membro da Equipe de Planejamento

Vanessa Covre Rangel Marques

Matrícula 140

Membro da Equipe de Planejamento



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 06/10/2025, às 13:39, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 06/10/2025, às 13:47, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 07/10/2025, às 09:20, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1052670** e o código CRC **0ABEFA74**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

Ao Pregoeiro,

Em atendimento ao CI, providenciamos exclusão do item 2.1.1 e ajuste do item 3.1.1, segue para demais providências quanto a publicação do certame.



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 06/10/2025, às 13:51, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1052754** e o código CRC **39901C18**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1052754



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

NLL - TERMO DE REFERENCIA DE TIC

Processo nº 9079618110000798.000048/2025-57

1. DEFINIÇÃO DO OBJETO

- 1.1. Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
- 1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.
- 1.3. O prazo de vigência da contratação é de 12 (doze) meses contados dos da assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.
- 1.3.1. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar;
- 1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual .

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

- 2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO

- 3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares

4. REQUISITOS DA CONTRATAÇÃO

4.1. Sustentabilidade

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.2. Garantia da contratação

4.2.1. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#), tendo em vista que o pagamento pelos serviços somente será realizado após a referida prestação e atesto pelo fiscal de contrato. Além disso, em caso de problema que se apresente posteriormente, o CRCES poderá instaurar procedimento administrativo sancionador com base na legislação vigente.

4.3. Vistoria

4.3.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo e-mail: administrativo@crc-es.org.br.

4.3.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

4.3.3. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.3.4. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.3.5. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.4. Local e horário da prestação dos serviços

4.4.1. Os serviços serão prestados na sede do CRCES, localizada na Rua Amélia da Cunha Ornelas, nº 30, Bairro Bento Ferreira, Vitória/ES – CEP: 29.050-620 Rotinas a serem cumpridas.

4.5. Materiais a serem disponibilizados

4.5.1. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário.

4.6. Informações relevantes para o dimensionamento da proposta

4.6.1. A Contratada deverá prestar serviços gerenciados de Tecnologia da Informação que abrangem o suporte técnico avançado (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a gestão de incidentes e mudanças. O escopo prevê a gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), com o fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, e a gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais. Será responsável também pelo monitoramento contínuo da infraestrutura, com identificação e mitigação proativa de riscos, pela manutenção preventiva e corretiva de todo o parque de TI, pela gestão e monitoramento dos links de internet, pela gestão e manutenção da infraestrutura hiperconvergente e do banco de dados em SQL Server. Além disso, inclui o fornecimento, instalação e gestão de um Firewall de Próxima Geração e a implementação e gestão de solução de backup local e em nuvem. Os serviços atenderão a única localidade do CRCES, até 60 estações de trabalho (físicas ou virtuais), 5 servidores físicos e 12 servidores virtuais.

4.6.2. A empresa contratada deverá estar plenamente capacitada para gerenciar toda a estrutura de TI híbrida do CRCES. Esta estrutura é complexa e inclui uma infraestrutura hiperconvergente (com

armazenamento baseado em Software-defined Storage - SDS), uma infraestrutura com acessos VDI (Virtual Desktop Infrastructure), máquinas virtuais e uma infraestrutura tradicional (com desktops físicos e notebooks).

4.6.3. A Contratada será responsável por assegurar a gestão completa dos backups e restores de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a disponibilidade e integridade dos dados em todas as plataformas.

4.7. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

4.7.1. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

4.8. Procedimentos de transição e finalização do contrato

4.8.1. Apresentar relatório final de atividades, contendo o resumo dos serviços executados, as ocorrências técnicas registradas, pendências identificadas e orientações para continuidade da operação da infraestrutura de TI, incluindo rede, segurança da informação, backup e suporte.

4.8.2. Entregar toda a documentação técnica e operacional produzida durante a execução do contrato, em meio físico e/ou digital, de forma organizada, classificada e atualizada, contemplando registros de configuração de equipamentos, scripts, inventários, diagramas de rede, manuais operacionais e demais documentos que garantam a rastreabilidade e integridade das informações

4.8.3. Transferir conhecimentos e informações relevantes ao(s) servidor(es) designado(s) pela Administração, por meio de reuniões técnicas, relatórios explicativos e capacitação operacional, com foco nos processos relacionados à infraestrutura de redes, segurança da informação, monitoramento e procedimentos de contingência

4.8.4. Assegurar a continuidade dos serviços durante eventual período de transição contratual, caso haja nova contratação em andamento, por prazo acordado com a Administração, a fim de garantir a operação ininterrupta dos serviços essenciais de tecnologia da informação.

4.8.5. Restituir, quando aplicável, equipamentos, materiais, documentos, credenciais, acessos a sistemas e demais bens disponibilizados pela contratante ao longo do contrato.

4.8.6. Emitir declaração formal de encerramento das obrigações contratuais, condicionada à aceitação pela fiscalização e à inexistência de pendências técnicas ou administrativas, comprovando a plena execução dos serviços contratados e a entrega dos produtos finais previstos. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

5. MODELO DE EXECUÇÃO DO OBJETO

5. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: 5 (cinco) dias da emissão da ordem de serviço;

5.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

5.1.3. Cronograma de realização dos serviços:

6. CARACTERÍSTICAS DA SOLUÇÃO:

6.1. ESTUDO DA SOLUÇÃO DE ACESSO VIA WI-FI.

6.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

6.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

6.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

6.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução.

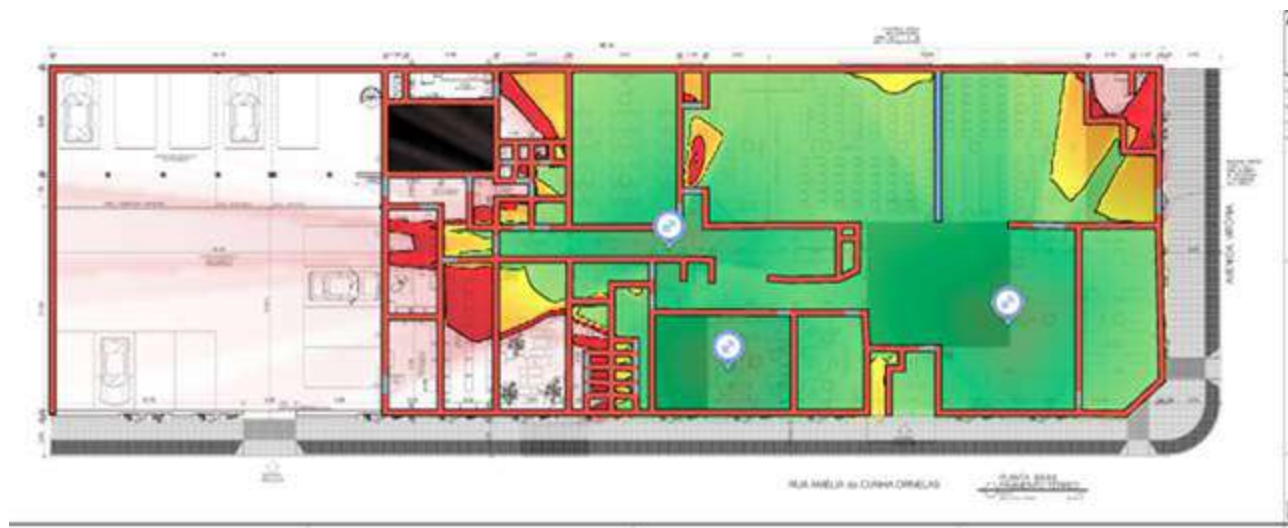
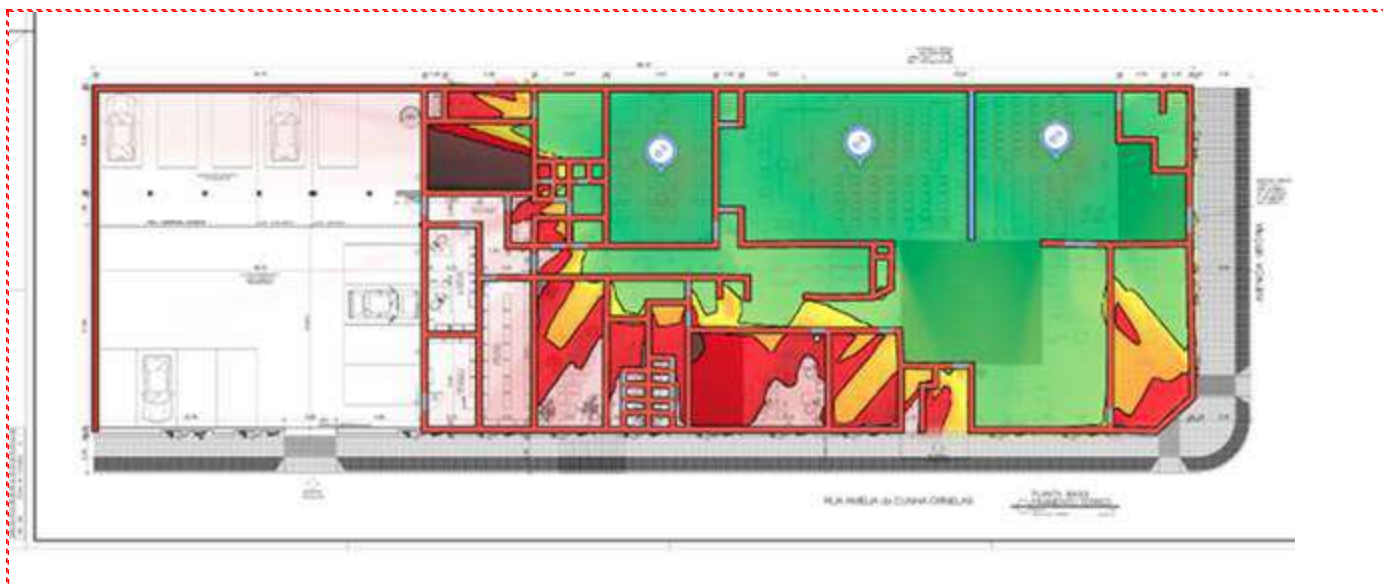
6.1.5. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

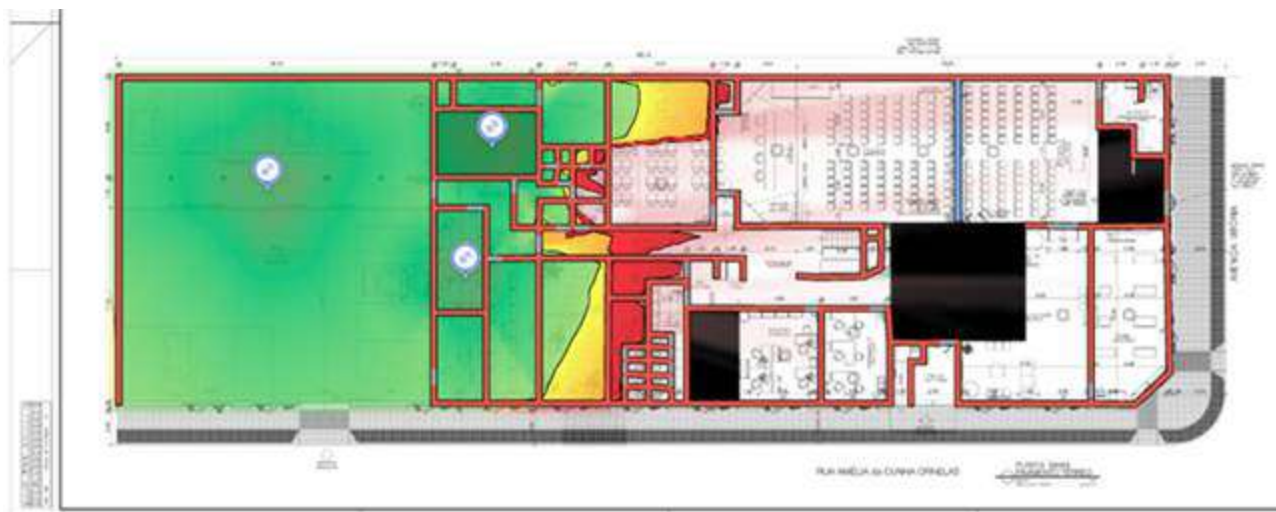
6.1.6. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.

6.2. Site Survey Preliminar

6.2.1. Para a definição da quantidade de equipamentos necessários, o CRCES realizou um levantamento de campo (site survey) preliminar, cujos resultados são apresentados a seguir:

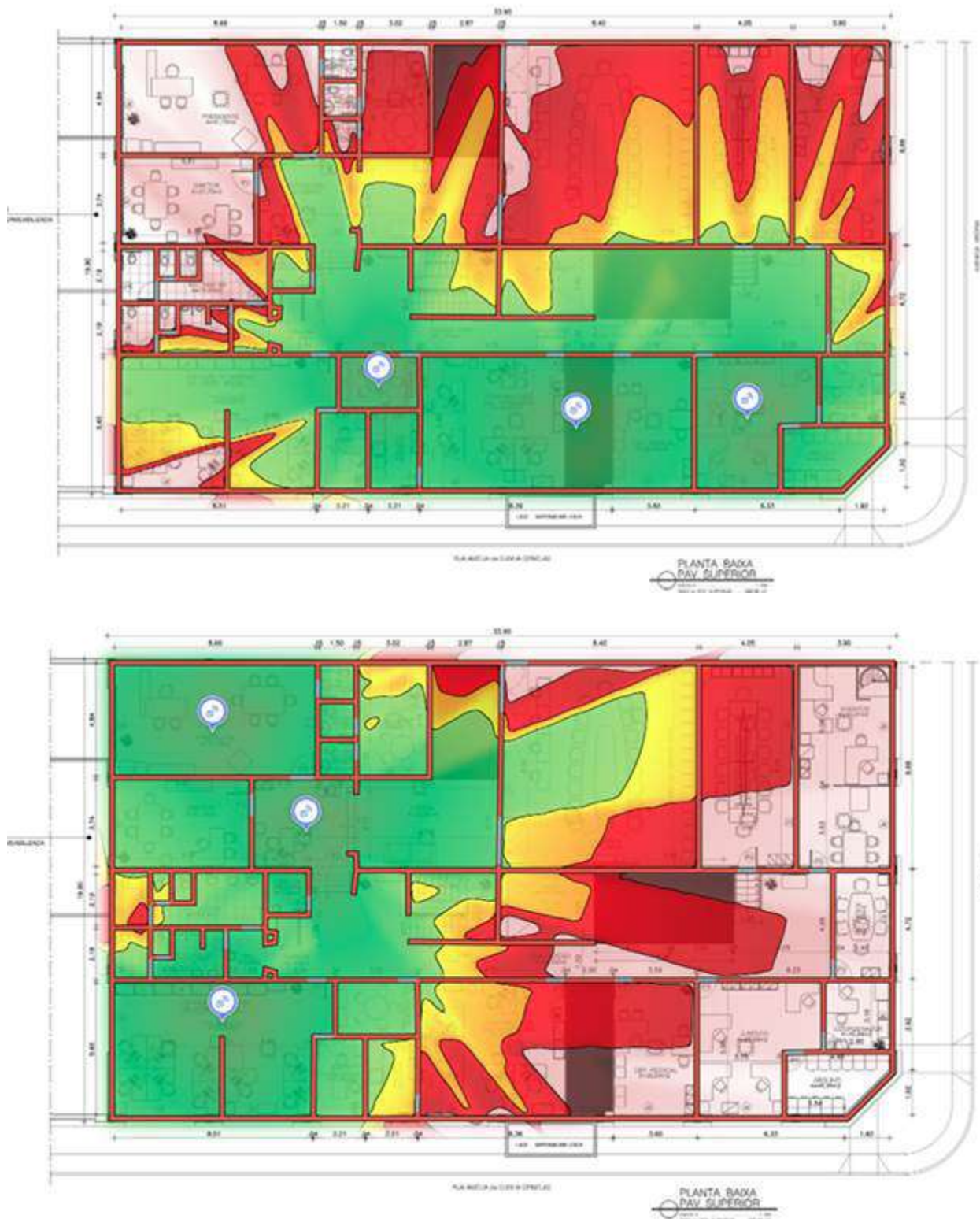
a) Pavimento térreo - 09 equipamentos





b) Pavimento superior - 09 equipamentos





6.2.2. ESTUDO DOS SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

6.2.2.1. Definição do objeto

6.2.2.2. Contratação de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial de acordo com a tabela abaixo:

TIPO	DESCRIÇÃO	QUANTIDADE
Virtualizador	Hyper-V	05
Servidor c/ Windows Server 2022	Dell PowerEdge R640	02
Servidor c/ Windows Server 2022	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01

Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01
Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados -VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson PowerLite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01
Solução de acesso à internet via Wi-Fi	Conforme item 1 do Termo de referência	
Solução de segurança FWaaS	Conforme item 2 do Termo de referência	
Solução de backup Cooperativo	Conforme item 3 do Termo de referência	

7. Definição dos itens.

ITEM	SUBITEM	CATSER	DESCRIÇÃO	DESCRIÇÃO COMPLEMENTAR	UNIDADE DE MEDIDA	QUANTIDADE
01	01	30710	SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.	Fornecimento e instalação de uma rede corporativa Wi-Fi completa.	Mês	12
	02	30736	SOLUÇÃO DE SEGURANÇA FWaaS	Instalação e gestão de Firewall de Próxima Geração, conforme termo de referência.	Mês	12
	03	30744	SOLUÇÃO DE BACKUP CORPORATIVO	Implementação e de solução de backup local e em nuvem.	Mês	12
	04	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1,N2 E N3	Suporte técnico avançado (remoto e presencial) conforme termo de referência	Mês	12

8. Descrição técnica dos itens:

8.1. SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.

8.1.1. Características da solução

8.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

8.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

8.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

8.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

8.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

8.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência.

8.1.2. Características dos pontos de acesso à internet via Wifi.

8.1.2.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

8.1.2.2. Deve ser compatível e gerenciado pelo equipamento que está incluso no ITEM “Solução de segurança FWaaS (Firewall como serviço). deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.1.2.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

8.1.2.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

8.1.2.5. Deve permitir ser gerenciado remotamente através de links WAN;

8.1.2.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

8.1.2.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

8.1.2.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

8.1.2.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

8.1.2.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

8.1.2.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

8.1.2.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

8.1.2.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

8.1.2.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

8.1.2.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

8.1.2.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

- 8.1.2.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
- 8.1.2.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 8.1.2.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 8.1.2.20. Deve permitir operação em modo Mesh;
- 8.1.2.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
- 8.1.2.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
- 8.1.2.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- 8.1.2.24. Deve suportar OFDMA;
- 8.1.2.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;
- 8.1.2.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 8.1.2.27. Deve suportar BSS Coloring;
- 8.1.2.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- 8.1.2.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;
- 8.1.2.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);
- 8.1.2.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;
- 8.1.2.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;
- 8.1.2.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
- 8.1.2.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 8.1.2.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
- 8.1.2.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- 8.1.2.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);
- 8.1.2.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
- 8.1.2.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.1.2.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 8.1.2.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 8.1.2.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

- 8.1.2.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.1.2.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 8.1.2.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 8.1.2.46. Deve implementar o padrão IEEE 802.11e;
- 8.1.2.47. Deve implementar o padrão IEEE 802.11h;
- 8.1.2.48. Deve implementar o padrão IEEE 802.3az;
- 8.1.2.49. Deve suportar ser gerenciado via SNMP;
- 8.1.2.50. Deve suportar consultas via REST API;
- 8.1.2.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
- 8.1.2.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
- 8.1.2.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- 8.1.2.54. Deve possuir indicadores luminosos (LED) para indicação de status;
- 8.1.2.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 8.1.2.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 8.1.2.57. Deve possuir certificado emitido pela Wi-Fi Alliance;
- 8.1.2.58. Deve estar homologado pela ANATEL na data de execução do pregão;
- 8.1.2.59. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.2.60. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.2.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.3. Características do equipamento controlador de pontos de acesso Wifi;

- 8.1.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 8.1.3.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
- 8.1.3.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- 8.1.3.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
- 8.1.3.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 8.1.3.6. Deve possuir 1 (uma) interface USB;
- 8.1.3.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);
- 8.1.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 8.1.3.9. Deve possuir tabela MAC com suporte a 32.000 endereços;
- 8.1.3.10. Deve operar com latência igual ou inferior à 1us (microsegundo);
- 8.1.3.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 8.1.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo

com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.1.3.13. Deve suportar a comutação de Jumbo Frames;

8.1.3.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

8.1.3.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

8.1.3.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.1.3.17. Deve implementar serviço de DHCP Relay;

8.1.3.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.1.3.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.1.3.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.1.3.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.1.3.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

8.1.3.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.1.3.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.1.3.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.1.3.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.1.3.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

8.1.3.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.1.3.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

8.1.3.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

8.1.3.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

8.1.3.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.1.3.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.1.3.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.1.3.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.1.3.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.1.3.37. Deve suportar MAC Authentication Bypass (MAB);

8.1.3.38. Deve implementar RADIUS CoA (Change of Authorization);

8.1.3.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

- 8.1.3.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 8.1.3.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
- 8.1.3.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 8.1.3.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 8.1.3.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 8.1.3.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 8.1.3.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 8.1.3.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 8.1.3.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 8.1.3.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 8.1.3.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 8.1.3.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 8.1.3.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 8.1.3.53. Deve permitir ser gerenciado através de IPv6;
- 8.1.3.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 8.1.3.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 8.1.3.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 8.1.3.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 8.1.3.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 8.1.3.59. Deverá suportar ser configurado e monitorado através de REST API;
- 8.1.3.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 8.1.3.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 8.1.3.62. Deve suportar temperatura de operação de até 45º Celsius;
- 8.1.3.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 8.1.3.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 8.1.3.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 8.1.3.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.3.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.3.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de

encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.1.4. Requisitos da instalação da solução de acesso à internet via Wi-Fi.

8.1.4.1. Implementação física.

8.1.4.1.1. Pontos de acesso:

8.1.4.1.1.1. Serviço de Implementação para rede WLAN8

8.1.4.1.1.2. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura 3 total, sendo observada a quantidade mínima estabelecida pela DTIC,

8.1.4.1.1.3. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;

8.1.4.1.1.4. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;

8.1.4.1.1.5. Requisitos gerais de Implantação

8.1.4.1.1.6. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.

8.1.4.1.1.7. Será realizada instalação física conforme a necessidade da contratante.

8.1.4.1.1.8. O ponto de acesso wifi deverá ser fixado no teto ou parede.

8.1.4.1.1.9. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

8.1.4.1.2. Controlador de pontos de acesso:

8.1.4.1.2.1. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;

8.1.4.1.2.2. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

8.1.4.1.3. Requisitos para instalação do cabeamento:

8.1.4.1.3.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;

8.1.4.1.3.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;

8.1.4.1.3.3. Conectorização e crimpagem dos cabos em ambos os extremos;

8.1.4.1.3.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;

8.1.4.1.3.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;

8.1.4.1.3.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;

8.1.4.1.3.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;

8.1.4.1.3.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

8.1.4.2. Implementação lógica.

8.1.4.2.1. Pontos de acesso:

8.1.4.2.1.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir

8.1.4.2.1.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

8.1.4.2.1.3. Cadastro das subscrições dos APs na plataforma de gerência;

8.1.4.2.1.4. Endereçamento e segmentação das Redes WIRELESS;

8.1.4.2.1.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e

policiamento de acordo com as aplicações a serem utilizadas na rede wireless);

- 8.1.4.2.1.6. Definição de políticas de bloqueio e permissão de acesso;
- 8.1.4.2.1.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.1.8. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.1.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 8.1.4.2.1.10. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.1.11. Configuração de Syslog, quando aplicável;
- 8.1.4.2.1.12. Configuração de redes locais (VLANs);
- 8.1.4.2.1.13. Configuração de redes locais (SSIDs);
- 8.1.4.2.1.14. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.1.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 8.1.4.2.1.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 8.1.4.2.1.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.18. Configurações de grupos de ponto de acesso;
- 8.1.4.2.1.19. Configuração de algoritmo de criptografia a ser utilizado;
- 8.1.4.2.1.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 8.1.4.2.1.22. Configuração de segurança de rede;
- 8.1.4.2.1.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 8.1.4.2.1.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 8.1.4.2.1.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;
- 8.1.4.2.1.26. Emissão de relatórios de implantação contendo:
- 8.1.4.2.1.27. Mapas de rede,
- 8.1.4.2.1.28. Relação de equipamentos implantados,
- 8.1.4.2.1.29. Configurações feitas nos softwares;
- 8.1.4.2.1.30. Resultado dos testes realizados;

8.1.4.2.2. Controlador de pontos de acesso:

- 8.1.4.2.2.1. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.2.2. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.2.3. Endereçamento IP;
- 8.1.4.2.2.4. Telnet, se necessário;
- 8.1.4.2.2.5. Secure Shell (SSH), se necessário;
- 8.1.4.2.2.6. Web (HTTP), se necessário;
- 8.1.4.2.2.7. Restrições (Filtros/ACLs) de Acesso;
- 8.1.4.2.2.8. Autenticação;
- 8.1.4.2.2.9. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.2.10. Configuração de redes locais (VLANs);
- 8.1.4.2.2.11. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.2.12. Configuração do protocolo Rapid Spanning Tree (RSTP);
- 8.1.4.2.2.13. Configuração de BPDU GUARD;
- 8.1.4.2.2.14. Configuração de Root Spanning Tree;
- 8.1.4.2.2.15. Interfaces de roteamento IP;
- 8.1.4.2.2.16. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;
- 8.1.4.2.2.17. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;
- 8.1.4.2.2.18. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.19. Otimização da Solução
- 8.1.4.2.2.20. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela

plataforma de gerenciamento unificado.

- 8.1.4.2.2.21. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.22. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;
- 8.1.4.2.2.23. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto
- 8.1.4.2.2.24. Ativação de recursos para o controle de broadcast storms;
- 8.1.4.2.2.25. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.26. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.27. Controle de acesso a rede através do padrão IEEE 802.1x;
- 8.1.4.2.2.28. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;
- 8.1.4.2.2.29. Configuração de DHCP Snooping;
- 8.1.4.2.2.30. Configuração de DHCP Relay;
- 8.1.4.2.2.31. Configuração de interface confiável (trust Interface);
- 8.1.4.2.2.32. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.
- 8.1.4.2.2.33. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;
- 8.1.4.2.2.34. Criação e ativação de regras de acesso e perfis de acesso à rede;
- 8.1.4.2.2.35. Configuração de parâmetros de qualidade de serviço (QoS);
- 8.1.4.2.2.36. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;
- 8.1.4.2.2.37. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;
- 8.1.4.2.2.38. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;
- 8.1.4.2.2.39. Ativação e teste das ACLs nos equipamentos fornecidos;
- 8.1.4.2.2.40. Homologação
- 8.1.4.2.2.41. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.
- 8.1.4.2.2.42. Documentação em formato PDF contendo os itens a seguir:
- 8.1.4.2.2.43. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.
- 8.1.4.2.2.44. Arquivos de configuração dos ativos de rede;
- 8.1.4.2.2.45. Backup das configurações dos softwares utilizados;
- 8.1.4.2.2.46. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega.

8.2. Solução de segurança FWaaS (Firewall como serviço).

8.2.1. Características da solução.

- 8.2.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
- 8.2.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
- 8.2.1.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
- 8.2.1.4. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
- 8.2.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o

pleno funcionamento da solução

8.2.1.6. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

8.2.1.7. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

8.2.1.8. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

8.2.2. Requisitos técnicos dos equipamentos que compõe a solução:

8.2.2.1. Características simplificadas:

8.2.2.1.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

8.2.2.1.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;

8.2.2.1.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;

8.2.2.1.4. Deve Suportar, no mínimo, 6,5 (Seis virgula cinco) Gbps de throughput VPN IPSec;

8.2.2.1.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;

8.2.2.1.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;

8.2.2.1.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;

8.2.2.1.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;

8.2.2.1.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.

8.2.2.1.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;

8.2.2.1.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;

8.2.2.1.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;

8.2.2.1.13. Deve possuir porta console RJ-45;

8.2.2.1.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;

8.2.2.1.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

8.2.2.1.16. Deve possuir Fontes redundantes.

8.2.2.1.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.

8.2.2.1.18. Deve ser licenciado para uso pelo período de duração do contrato.

8.2.2.1.19. Deve possuir garantia para uso pelo período de duração do contrato.

8.2.2.1.20. Firewalls de próxima geração (NGFW):

8.2.2.1.21. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

8.2.2.1.22. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

8.2.2.1.23. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8.2.2.1.24. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional

de todos os recursos;

8.2.2.1.25. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

8.2.2.1.26. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

8.2.2.2. Funcionalidades de rede e firewall:

8.2.2.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.2.2.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

8.2.2.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.2.2.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

8.2.2.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.2.2.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

8.2.2.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.2.2.2.8. Deverá suportar sFlow ou Netflow;

8.2.2.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.2.2.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

8.2.2.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.2.2.2.12. Deve implementar o protocolo ECMP;

8.2.2.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.2.2.2.14. Enviar log para sistemas de monitoração externos;

8.2.2.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

8.2.2.2.16. Deve possuir mecanismos de proteção anti-spoofing;

8.2.2.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

8.2.2.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

8.2.2.2.19. Suportar OSPF graceful restart;

8.2.2.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

8.2.2.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

8.2.2.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

8.2.2.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.2.2.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

8.2.2.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

8.2.2.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

8.2.2.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

8.2.2.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

8.2.2.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails,

notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

8.2.2.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

8.2.2.2.31. Deverá suportar controle por zonas de segurança;

8.2.2.2.32. Deverá suportar controles de políticas por porta e protocolo;

8.2.2.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.2.2.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.2.2.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.2.2.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.2.2.2.37. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.2.2.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.2.2.2.39. Suporte a objetos e regras IPV6;

8.2.2.2.40. Suporte a objetos e regras multicast;

8.2.2.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

8.2.2.2.42. Funcionalidade de controle de aplicações:

8.2.2.2.43. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

8.2.2.2.44. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.2.2.2.45. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

8.2.2.2.46. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

8.2.2.2.47. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

8.2.2.2.48. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

8.2.2.2.49. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

8.2.2.2.50. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

8.2.2.2.51. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

8.2.2.2.52. Identificar o uso de táticas evasivas via comunicações criptografadas;

8.2.2.2.53. Atualizar a base de assinaturas de aplicações automaticamente;

8.2.2.2.54. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

8.2.2.2.55. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

8.2.2.2.56. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

8.2.2.2.57. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de

aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

8.2.2.2.58. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

8.2.2.2.59. Deve alertar o usuário quando uma aplicação for bloqueada;

8.2.2.2.60. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.61. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.62. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

8.2.2.2.63. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

8.2.2.2.64. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

8.2.2.2.65. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

8.2.2.2.66. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

8.2.2.2.67. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

8.2.2.2.68. Funcionalidade de prevenção de intrusão de ameaças:

8.2.2.2.69. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

8.2.2.2.70. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.2.2.2.71. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.2.2.2.72. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e “quarentenar” IP do atacante por um intervalo de tempo;

8.2.2.2.73. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

8.2.2.2.74. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.2.2.2.75. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.2.2.2.76. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.2.2.2.77. Deve permitir o bloqueio de vulnerabilidades;

8.2.2.2.78. Deve permitir o bloqueio de exploits conhecidos;

8.2.2.2.79. Deve incluir proteção contra-ataques de negação de serviços;

8.2.2.2.80. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

8.2.2.2.81. Detectar e bloquear a origem de portscans;

8.2.2.2.82. Bloquear ataques efetuados por worms conhecidos;

8.2.2.2.83. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

8.2.2.2.84. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.2.2.2.85. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

8.2.2.2.86. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

8.2.2.2.87. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

8.2.2.2.88. Identificar e bloquear comunicação com botnets;

8.2.2.2.89. Registrar na console de monitoração as seguintes informações sobre ameaças

identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.2.2.2.90. Os eventos devem identificar o país de onde partiu a ameaça;

8.2.2.2.91. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

8.2.2.2.92. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

8.2.2.2.93. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

8.2.2.2.94. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

8.2.2.2.95. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

8.2.2.2.96. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

8.2.2.2.97. Funcionalidade de filtro de conteúdo web e dns:

8.2.2.2.98. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

8.2.2.2.99. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

8.2.2.2.100. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.2.2.2.101. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

8.2.2.2.102. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.2.2.2.103. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

8.2.2.2.104. Possuir pelo menos 70 (setenta) categorias de URLs;

8.2.2.2.105. Deve possuir a função de exclusão de URLs do bloqueio;

8.2.2.2.106. Permitir a customização de página de bloqueio;

8.2.2.2.107. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

8.2.2.2.108. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

8.2.2.2.109. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

8.2.2.2.110. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

8.2.2.2.111. Funcionalidade de identificação de usuários:

8.2.2.2.112. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

8.2.2.2.113. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

8.2.2.2.114. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

8.2.2.2.115. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários,

- suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 8.2.2.2.116. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.2.2.2.117. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 8.2.2.2.118. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 8.2.2.2.119. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 8.2.2.2.120. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 8.2.2.2.121. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 8.2.2.2.122. Funcionalidade de filtro de dados:
- 8.2.2.2.123. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 8.2.2.2.124. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.125. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.126. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
- 8.2.2.2.127. Funcionalidade de geolocalização:
- 8.2.2.2.128. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 8.2.2.2.129. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 8.2.2.2.130. Funcionalidade de vpn.
- 8.2.2.2.131. Suportar VPN Site-to-Site e Cliente-To-Site;
- 8.2.2.2.132. Suportar IPSec VPN;
- 8.2.2.2.133. A VPN IPSEC deve suportar 3DES;
- 8.2.2.2.134. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 8.2.2.2.135. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 8.2.2.2.136. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 8.2.2.2.137. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 8.2.2.2.138. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 8.2.2.2.139. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 8.2.2.2.140. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 8.2.2.2.141. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 8.2.2.2.142. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 8.2.2.2.143. Atribuição de DNS nos clientes remotos de VPN;
- 8.2.2.2.144. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 8.2.2.2.145. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 8.2.2.2.146. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 8.2.2.2.147. Deverá manter uma conexão segura com o portal durante a sessão;
- 8.2.2.2.148. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
- 8.2.2.2.149. Funcionalidade de qos, traffic shaping e priorização de tráfego;
- 8.2.2.2.150. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo,

(como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

8.2.2.2.151. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

8.2.2.2.152. Endereço de origem e Endereço de destino;

8.2.2.2.153. Usuário e grupo;

8.2.2.2.154. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.2.2.2.155. Por porta;

8.2.2.2.156. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

8.2.2.2.157. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

8.2.2.2.158. O QoS deve possibilitar a definição de fila de prioridade;

8.2.2.2.159. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

8.2.2.2.160. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

8.2.2.2.161. Suportar modificação de valores DSCP para o Diffserv;

8.2.2.2.162. Suportar priorização de tráfego usando informação de ToS (Type of Service);

8.2.2.2.163. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

8.2.2.2.164. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

8.2.2.2.165. Deve possibilitar a definição de bandas distintas para download e upload;

8.2.2.2.166. Funcionalidade de balanceamento inteligente de links;

8.2.2.2.167. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

8.2.2.2.168. A solução deve ser capaz de agregar vários links em uma interface virtual;

8.2.2.2.169. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

8.2.2.2.170. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

8.2.2.2.171. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

8.2.2.2.172. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

8.2.2.2.173. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

8.2.2.2.174. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

8.2.2.2.175. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

8.2.2.2.176. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

8.2.2.2.177. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface

está conectada;

8.2.2.2.178. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

8.2.2.2.179. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

8.2.2.2.180. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

8.2.2.2.181. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

8.2.2.2.182. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

8.2.2.2.183. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

8.2.2.2.184. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

8.2.2.2.185. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

8.2.2.2.186. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

8.2.2.2.187. A solução deve suportar nativamente conectores com clouds públicas;

8.2.2.2.188. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

8.2.2.2.189. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

8.2.2.2.190. Deve implementar balanceamento de link por hash do IP de origem;

8.2.2.2.191. Deve implementar balanceamento de link por hash do IP de origem e destino;

8.2.2.2.192. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

8.2.2.2.193. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

8.2.2.2.194. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

8.2.2.2.195. Funcionalidade de controlador de rede sem fio:

8.2.2.2.196. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

8.2.2.2.197. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

8.2.2.2.198. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

8.2.2.2.199. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

8.2.2.2.200. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

8.2.2.2.201. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de

canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

8.2.2.2.202. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

8.2.2.2.203. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

8.2.2.2.204. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.2.2.2.205. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.2.2.2.206. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.2.2.2.207. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

8.2.2.2.208. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

8.2.2.2.209. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

8.2.2.2.210. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.2.2.2.211. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.2.2.2.212. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

8.2.2.2.213. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

8.2.2.2.214. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

8.2.2.2.215. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

- 8.2.2.2.216. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 8.2.2.2.217. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 8.2.2.2.218. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 8.2.2.2.219. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 8.2.2.2.220. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 8.2.2.2.221. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 8.2.2.2.222. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.2.2.2.223. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 8.2.2.2.224. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 8.2.2.2.225. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
- 8.2.2.2.226. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 8.2.2.2.227. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 8.2.2.2.228. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
- 8.2.2.2.229. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
- 8.2.2.2.230. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
- 8.2.2.2.231. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
- 8.2.2.2.232. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;
- 8.2.2.2.233. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
- 8.2.2.2.234. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
- 8.2.2.2.235. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

- 8.2.2.2.236. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 8.2.2.2.237. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
- 8.2.2.2.238. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 8.2.2.2.239. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
- 8.2.2.2.240. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- 8.2.2.2.241. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.2.2.2.242. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 8.2.2.2.243. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 8.2.2.2.244. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 8.2.2.2.245. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 8.2.2.2.246. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 8.2.2.2.247. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 8.2.2.2.248. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 8.2.2.2.249. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 8.2.2.2.250. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 8.2.2.2.251. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 8.2.2.2.252. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 8.2.2.2.253. A solução deve permitir a configuração do captive portal com endereço IPv6;
- 8.2.2.2.254. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 8.2.2.2.255. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 8.2.2.2.256. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 8.2.2.2.257. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 8.2.2.2.258. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
- 8.2.2.2.259. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 8.2.2.2.260. A solução deve permitir que os usuários sejam capazes de acessar serviços

disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

8.2.2.2.261. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

8.2.2.2.262. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

8.2.2.2.263. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

8.2.2.2.264. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

8.2.2.2.265. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

8.2.2.2.266. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

8.2.2.2.267. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

8.2.2.2.268. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

8.2.2.2.269. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

8.2.2.2.270. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

8.2.2.2.271. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

8.2.2.2.272. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

8.2.2.2.273. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

8.2.2.2.274. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

8.2.2.2.275. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

8.2.2.2.276. A solução deve possuir ferramentas de diagnósticos e debug;

8.2.2.2.277. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

8.2.2.2.278. A solução deve suportar comunicação com elementos externos através de REST API;

8.2.2.2.279. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

8.2.2.2.280. Funcionalidade de controlador de rede cabeada:

8.2.2.2.281. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

8.2.2.2.282. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

8.2.2.2.283. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

8.2.2.2.284. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

8.2.2.2.285. Deve montar a topologia da rede de maneira automática;

8.2.2.2.286. Deve ser capaz de configurar os switches da rede;

8.2.2.2.287. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

- 8.2.2.2.288. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 8.2.2.2.289. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 8.2.2.2.290. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 8.2.2.2.291. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 8.2.2.2.292. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 8.2.2.2.293. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard,;
- 8.2.2.2.294. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 8.2.2.2.295. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 8.2.2.2.296. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 8.2.2.2.297. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 8.2.2.2.298. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 8.2.2.2.299. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 8.2.2.2.300. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 8.2.2.2.301. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 8.2.2.2.302. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 8.2.2.2.303. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 8.2.2.2.304. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

8.2.3. Requisitos da instalação da Solução de segurança FWaaS (Firewall como serviço)

8.2.3.1. Implementação Física:

- 8.2.3.1.1. Levantamento de toda estrutura física do ambiente;
- 8.2.3.1.2. Levantamento da estrutura Elétrica;
- 8.2.3.1.3. Verificação do espaço a ser instalado os equipamentos;
- 8.2.3.1.4. Abertura e conferência das caixas dos equipamentos;
- 8.2.3.1.5. Fixação do equipamento no RACK;
- 8.2.3.1.6. Conexão da fonte de alimentação elétrica em réguas de tomada;
- 8.2.3.1.7. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;
- 8.2.3.1.8. Conexão das interfaces de rede com os switches;

8.2.3.2. Implementação lógica:

- 8.2.3.2.1. Parametrização do Licenciamento;
- 8.2.3.2.2. Parametrização das interfaces de rede;
- 8.2.3.2.3. Atualização da última versão de Firmware;
- 8.2.3.2.4. Parametrização das regras de NAT;
- 8.2.3.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 8.2.3.2.6. Parametrização de Controle de Aplicação;
- 8.2.3.2.7. Parametrização de VPN (Virtual Private Network);
- 8.2.3.2.8. Parametrização IDS/IPS;
- 8.2.3.2.9. Parametrização DNS;
- 8.2.3.2.10. Parametrização de Gateway Antivírus;

- 8.2.3.2.11. Parametrização de Objetos de Endereço;
- 8.2.3.2.12. Parametrização de Grupo de Objetos;
- 8.2.3.2.13. Parametrização de Load Balancing;
- 8.2.3.2.14. Parametrização de SSO (Single Sign-on);
- 8.2.3.2.15. Parametrização de SNMP;
- 8.2.3.2.16. Parametrização de NTP;
- 8.2.3.2.17. Parametrização de PortGroups;
- 8.2.3.2.18. Parametrização de Zones;
- 8.2.3.2.19. Parametrização de Serviços;
- 8.2.3.2.20. Parametrização de Rotas;
- 8.2.3.2.21. Parametrização de DHCP

8.3. SOLUÇÃO DE BACKUP CORPORATIVO

8.3.1. Características do Software de Backup

- 8.3.1.1. Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- 8.3.1.2. Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.
- 8.3.1.3. Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- 8.3.1.4. Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.
- 8.3.1.5. Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.
- 8.3.1.6. Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- 8.3.1.7. Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.
- 8.3.1.8. Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.
- 8.3.1.9. Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.
- 8.3.1.10. Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.
- 8.3.1.11. Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.
- 8.3.1.12. Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.
- 8.3.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações: O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.
- 8.3.1.14. Backup Incremental e Diferencial: Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.
- 8.3.1.15. Cópias de Backup Imutáveis: Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.
- 8.3.1.16. Retenção Personalizável: O software deve oferecer flexibilidade na configuração de políticas

de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.

8.3.1.17. Arquivamento Inteligente: Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.

8.3.1.18. Monitoramento e Alertas: O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.

8.3.1.19. Dashboard Intuitivo: Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.

8.3.1.20. Otimização de Recursos (IOPS e Throughput): O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.

8.3.1.21. Restauração Granular: Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.

8.3.1.22. Recuperação Bare-Metal: Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.

8.3.1.23. Testes de Restauração Automática: Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.

8.3.1.24. Integração Nativa com Provedores de Nuvem: Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.

8.3.1.25. Economia de Largura de Banda: Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.

8.3.1.26. Perfis de Acesso Personalizáveis: O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.

8.3.1.27. Controle de Acessos Granular: Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.

8.3.1.28. Suporte a LGPD e Outras Normas: O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.

8.3.1.29. Auditorias e Relatórios: Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.

8.3.1.30. Automatização de trabalhos de Backup: Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.

8.3.1.31. Integração com Ferramentas de Orquestração: Suporte para integração com ferramentas

8.3.1.32. de orquestração e automação (ex: scripts PowerShell, APIs).

8.3.1.33. Cobertura Completa: O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.

8.3.1.34. Recuperação Granular: Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.

8.3.1.35. Agendamento e Automação: A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

8.3.2. Características do backup local:

8.3.2.1. A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.

8.3.2.2. Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.

8.3.3. Características do backup em nuvem:

- 8.3.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.
- 8.3.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.
- 8.3.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.
- 8.3.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
- 8.3.3.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.
- 8.3.3.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.
- 8.3.3.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.
- 8.3.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.
- 8.3.3.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.
- 8.3.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).
- 8.3.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.
- 8.3.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.
- 8.3.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.
- 8.3.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.
- 8.3.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.
- 8.3.3.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.
- 8.3.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.
- 8.3.3.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.
- 8.3.3.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.
- 8.3.3.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).
- 8.3.3.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.
- 8.3.3.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e

possíveis falhas.

8.3.3.23. Ferramentas de monitoramento nativas devem estar integradas.

8.3.3.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

8.3.4. Requisitos da instalação da Solução de Backup corporativo:

8.3.4.1. Implementação Física:

8.3.4.1.1. Verificar a estrutura elétrica do equipamento fornecido pelo CRC;

8.3.4.1.2. Verificar a conexão da fonte de alimentação elétrica em régua de tomada;

8.3.4.1.3. Verificar a conexão das interfaces de rede com os switches;

8.3.4.2. Implementação lógica.

8.3.4.2.1. Configurar o sistema de armazenamento local do equipamento, devendo:

8.3.4.2.1.1. Criar e configurar o arranjo de discos em RAID 5;

8.3.4.2.1.2. Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);

8.3.4.2.1.3. Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas; Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.

8.3.4.2.1. Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:

8.3.4.2.2.1. Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;

8.3.4.2.2.2. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

8.4. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

8.4.1. Definição do objeto

8.4.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, firewall, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

8.4.1.2. O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21 da Lei nº 14.133, de 2021.

8.4.1.3. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail administrativo@crces.org.br.

8.4.1.4. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

8.4.1.5. A contratada deverá:

8.4.1.5.1. Monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

8.4.1.5.2. Gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos

8.4.1.5.3. Possuir sistema de abertura de chamados pela internet.

8.4.1.5.4. Monitorar latência e uptime dos links configurados.

8.4.1.6. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

8.4.1.7. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela

empresa comprovando sua habilitação para a realização da vistoria.

8.4.2. Características do serviço prestado.

8.4.2.1. Monitoramento e suporte técnico:

- 8.4.2.1.1. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;
- 8.4.2.1.2. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:
- 8.4.2.1.3. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);
- 8.4.2.1.4. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;
- 8.4.2.1.5. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;
- 8.4.2.1.6. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

8.4.2.2. Serviços ambiente Legado:

8.4.2.2.1. Manutenção, gestão de ativos e rede:

- 8.4.2.2.1.1. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados na “Tabela do parque de informática do CRCES”;
- 8.4.2.2.1.2. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;
- 8.4.2.2.1.3. Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.
- 8.4.2.2.1.4. Executar a gestão técnica da infraestrutura de rede, abrangendo:
- 8.4.2.2.1.5. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;
- 8.4.2.2.1.6. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;
- 8.4.2.2.1.7. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;
- 8.4.2.2.1.8. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.
- 8.4.2.2.1.9. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

8.4.2.2.2. Serviços gerenciados:

- 8.4.2.2.2.1. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;
- 8.4.2.2.2.2. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;
- 8.4.2.2.2.3. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;
- 8.4.2.2.2.4. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

8.4.2.2.3. Controle, inventário e chamados:

- 8.4.2.2.3.1. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;
- 8.4.2.2.3.2. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

8.4.2.2.4. Logística e apoio à contratação:

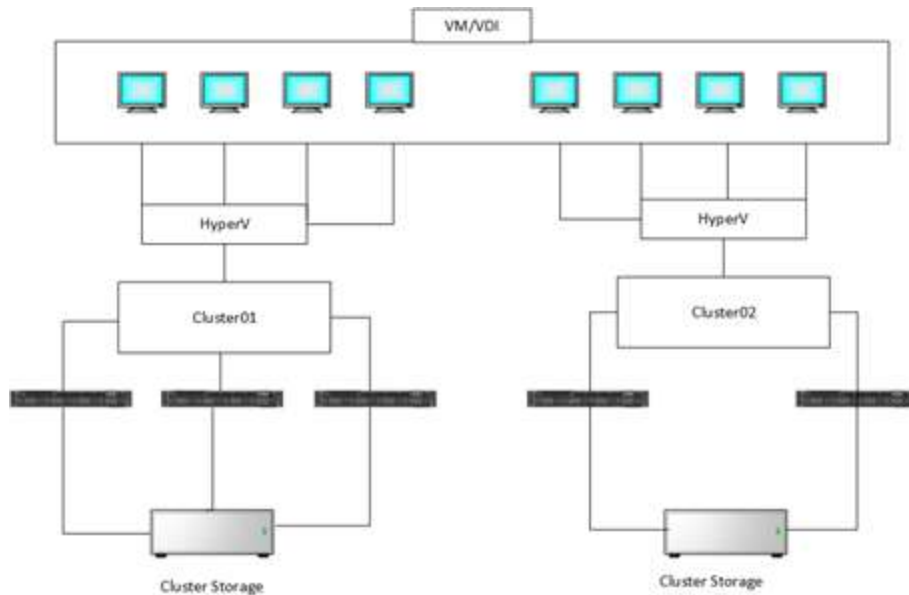
- 8.4.2.2.4.1. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;
- 8.4.2.2.4.2. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:
- 8.4.2.2.4.3. Elaboração de especificações técnicas;
- 8.4.2.2.4.4. Análise de propostas técnicas;
- 8.4.2.2.4.5. Apoio em processos licitatórios;
- 8.4.2.2.4.6. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

8.4.2.2.5. Atendimento presencial:

8.4.2.2.5.1. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 6 (seis) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

8.4.3. Tabela do parque de informática do CRCES:

8.4.3.1. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:



8.4.4. Manutenção preventiva e corretiva.

8.4.4.1. Manutenção Preventiva:

8.4.4.1.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

8.4.4.1.2. Tais atividades incluem, mas não se limitam a:

8.4.4.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

8.4.4.1.2.2. Limpeza técnica interna e externa;

8.4.4.1.2.3. Aferição e calibração de dispositivos, quando aplicável;

8.4.4.1.2.4. Atualização de firmwares, BIOS e softwares;

8.4.4.1.2.5. Verificação e otimização de configurações;

8.4.4.1.2.6. Avaliação do desempenho geral e análise de logs;

8.4.4.1.2.7. Testes de funcionalidade e conectividade.

8.4.4.1.2.8. Realizar monitoramento contínuo do sistema de backup local, incluindo:

8.4.4.1.2.8.1. Acompanhamento da integridade dos discos e volumes lógicos;

8.4.4.1.2.8.2. Monitoramento do uso de espaço em disco e alertas proativos;

8.4.4.1.2.8.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

8.4.4.1.3. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.

8.4.4.1.4. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.

8.4.4.1.5. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.

8.4.4.1.6. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que

solicitado.

8.4.4.2. Manutenção Corretiva:

8.4.4.2.1. Em caso de surgimento de problema técnico em qualquer um dos equipamentos ou serviços listados no item de manutenção preventiva a contratada deverá providenciar laudo técnico e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.

8.4.4.2.2. CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.

8.4.4.2.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.

8.4.4.2.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.

8.4.4.2.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.

8.4.4.2.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 dias úteis após o recebimento dos novos equipamentos/peças.

8.4.4.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.

8.4.4.2.8. Durante a execução do serviço externo, a empresa contratada deverá:

8.4.4.2.9. Se responsabilizar pelo transporte dos equipamentos que serão retirados;

8.4.4.2.10. Providenciar termo de responsabilidade de retirada;

8.4.4.2.11. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

8.4.4.2.12. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;

8.4.4.2.13. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;

8.4.4.2.14. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;

8.4.4.2.15. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;

8.4.4.2.16. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto à qualidade do produto entregue;

8.4.4.2.17. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.

8.4.5.2. Suporte para o item 2 “SOLUÇÃO DE SEGURANÇA FWaaS”:

8.4.5.2.1. Serviço Continuado

8.4.5.2.1.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;

8.4.5.2.1.2. Efetuar toda rotina de backup das configurações semanalmente;

8.4.5.2.1.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

8.4.5.2.1.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

- 8.4.5.2.1.5. Atividades relativas à Solução de Segurança:
- 8.4.5.2.1.6. Criação das rotas para links.
- 8.4.5.2.1.7. Criação de NAT.
- 8.4.5.2.1.8. Liberação de portas.
- 8.4.5.2.1.9. Configuração do Filtro de Conteúdo.
- 8.4.5.2.1.10. Configuração do Controle de Aplicativos.
- 8.4.5.2.1.11. Configuração do Agente para autenticação LDAP.
- 8.4.5.2.1.12. Configuração para o Single Sign-On (SSO).
- 8.4.5.2.1.13. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 8.4.5.2.1.14. Configuração de VPN client to site.
- 8.4.5.2.1.15. Configuração de VPN site to site.
- 8.4.5.2.1.16. Criação de regras de Firewall.
- 8.4.5.2.1.17. Criação de regras de QoS.
- 8.4.5.2.1.18. Emitir relatório de segurança mensal por localidade.
- 8.4.5.2.1.19. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 8.4.5.2.1.20. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.
- 8.4.5.2.1.21. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

8.4.5.3. Suporte para o item 3 “SOLUÇÃO DE BACKUP CORPORATIVO”

8.4.5.3.1. Serviço Continuado

- 8.4.5.3.1.1. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:
- 8.4.5.3.1.2. Acompanhamento da integridade dos discos e volumes lógicos;
- 8.4.5.3.1.3. Monitoramento do uso de espaço em disco e alertas proativos;
- 8.4.5.3.1.4. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.
- 8.4.5.3.1.5. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:
- 8.4.5.3.1.6. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;
- 8.4.5.3.1.7. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).
- 8.4.5.3.1.8. Deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:
- 8.4.5.3.1.9. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;
- 8.4.5.3.1.10. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;
- 8.4.5.3.1.11. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;
- 8.4.5.3.1.12. Ajustar as políticas de backup e monitoramento para o novo ambiente.
- 8.4.5.3.1.13. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

8.4.5.4. SLA dos serviços e atendimento

- 8.4.5.4.1. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 8.4.5.4.2. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 8.4.5.4.3. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

8.4.5.4.4. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

Níveis de Severidade

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

8.4.5.4.5. Descrição de atendimento para cada nível de severidade:

8.4.5.4.5.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

8.4.5.4.5.2. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

8.4.5.4.5.2.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

8.4.5.4.5.2.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.4.5.3. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.3.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

8.4.5.4.5.3.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.4.5.4. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.4.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

8.4.5.4.5.4.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

8.4.5.5. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

8.4.5.4.5.5. A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

8.4.5.4.5.6. Não poderá haver limites no quantitativo de abertura de chamados.

9. MODELO DE GESTÃO DO CONTRATO

9.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

9.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

9.4. O CRCES poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

9.5. Após a assinatura do contrato, o CRCES poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

9.6. Preposto

9.6.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

9.6.2. Fiscalização

9.6.3. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

9.6.4. O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

9.6.5. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

9.6.6. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

9.6.7. O fiscal do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

9.6.8. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

9.6.9. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

9.6.10. O fiscal do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

9.6.11. Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as

providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

9.6.12. Gestor do Contrato

9.6.13. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

9.6.14. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

9.6.15. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

9.6.16. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

9.6.17. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

9.6.18. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

9.6.19. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

10. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

10.1. A avaliação da execução do objeto utilizará o relatório/checklist para atesto de notas fiscais para aferição da qualidade da prestação do serviço.

10.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

10.1.1.1. não produzir os resultados acordados,

10.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

10.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

10.1.1.4. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

10.1.1.5. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

10.1.1.6. A avaliação da execução do objeto será conduzida utilizando o instrumento de verificação de conformidade, em conformidade com as especificações técnicas estabelecidas no item 5.

10.2. Do recebimento

10.2.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133, de 2021 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

10.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança

oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

10.2.3. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências. (Art. 22 e 23, X, Decreto nº 11.246, de 2022).

10.2.4. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

10.2.5. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

10.2.6. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

10.2.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

10.2.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

10.2.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as

10.2.10. especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

10.2.11. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

10.2.12. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

10.2.13. Emitir documento comprobatório da avaliação realizada pelos fiscais, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

10.2.14. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

10.2.15. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

10.2.16. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021 , comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

10.2.17. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

10.2.18. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

10.2.19. Liquidação

10.2.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de cinco dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

10.2.21. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

10.2.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

10.2.22.1. o prazo de validade;

10.2.22.2. a data da emissão;

10.2.22.3. os dados do contrato e do órgão contratante;

10.2.22.4. o período respectivo de execução do contrato;

10.2.22.5. o valor a pagar; e

10.2.22.6. eventual destaque do valor de retenções tributárias cabíveis.

10.2.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

10.2.24. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da

10.2.25. regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

10.2.26. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

10.2.27. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

10.2.28. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

10.2.29. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

10.2.30. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

10.3. Prazo de pagamento

10.3.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

10.4. Forma de pagamento

10.4.1. O pagamento será realizado preferencialmente por meio de chave pix indicada pelo fornecedor, desde que a conta para pagamento esteja em nome da empresa contratada, ou através de boleto/fatura emitido por este.

10.4.1.1. Na impossibilidade de pagamento via chave pix ou boleto/fatura, o valor poderá ser transferido para conta bancária, desde que a mesma esteja em nome da empresa contratada.

10.4.1.2. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

10.4.2. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

10.4.3. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

11.1. Forma de seleção e critério de julgamento da proposta.

11.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

11.2. Regime de execução

11.2.1. O regime de execução do objeto será empreitada por preço global.

11.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

11.3.1. Habilitação jurídica

11.3.1.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.3.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

11.3.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.4. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

11.3.1.5. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

11.3.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

11.3.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.3.1.9. Exigências Adicionais para Cooperativas

11.3.1.10. Caso a empresa participante seja uma cooperativa, deverá apresentar, além dos itens anteriores, a seguinte documentação complementar:

11.3.1.11. Relação de cooperados que atenderão o contrato, com atas de inscrição e comprovação de domicílio na localidade da sede da cooperativa.

11.3.1.12. Declaração de Regularidade de Situação do Contribuinte Individual (DRSCI) para cada um dos cooperados.

11.3.1.13. Comprovação do capital social proporcional ao número de cooperados necessários à execução do contrato.

11.3.1.14. Registro previsto na Lei nº 5.764, de 1971.

11.3.1.15. Comprovação de integração das quotas-partes dos cooperados que executarão o contrato.

11.3.1.16. Documentos de regularidade jurídica da cooperativa: ata de fundação, estatuto social, regimento dos fundos, editais e registros das últimas assembleias, além da ata que autorizou a participação na licitação.

11.3.1.17. Última auditoria contábil-financeira ou declaração de que a auditoria não foi exigida pelo órgão fiscalizador.

11.3.1.18. Modelo de gestão operacional, conforme a IN SEGES/ME nº 05/2017.

11.3.2. Habilitação fiscal, social e trabalhista

11.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

11.3.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.3.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.3.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.3.2.5. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.6. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.7. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

11.3.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.3.3. Qualificação Econômico-Financeira

11.3.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

11.3.4. Qualificação Técnica

Para a qualificação técnica, a empresa deverá cumprir os seguintes requisitos:

11.3.4.1. Requisitos de Capacidade Técnica da Empresa

11.3.4.1.1. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

11.3.4.1.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

- a) Serviços de backup em nuvem com, no mínimo, 25 terabytes de capacidade de armazenamento utilizável.
- b) Gestão de ambientes com infraestrutura virtualizada e VDI (Virtual Desktop Infrastructure) com pelo menos 30 estações virtuais.
- c) Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos.
- d) Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS).
- e) Hiperconvergência: Implementação, operação e manutenção de infraestruturas hiperconvergentes, com conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- f) Gerenciamento de Clusters de Servidores: Expertise em balanceamento de carga, otimização de recursos, failover e alta disponibilidade.
- g) Virtualização com Hyper-V: Conhecimento avançado em provisionamento, gerenciamento de imagens e otimização de desempenho de desktops virtuais.
- h) Administração de Banco de Dados SQL: Otimização de desempenho, segurança, backup e recuperação de desastres.
- i) Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação para garantir alta disponibilidade.

11.3.4.1.2. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única

contratação.

11.3.4.1.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

11.3.4.1.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

11.3.4.2. Qualificação Técnico-Profissional

11.3.4.2.1. Apresentação do(s) profissional(is), abaixo indicado(s), detentor(es) dos certificados abaixo indicado(s):

a) Certificação em tecnologias de firewall e segurança de rede, como Fortinet, Palo Alto ou Cisco.

b) ITIL v3 ou superior.

c) MCSA Windows Server 2012 ou superior.

d) Certificação para Instalação e Configuração de Switches DELL ou similar.

11.3.4.3. O(s) profissional(is) acima indicado(s) deverá(ão) participar do serviço objeto do contrato, e será admitida a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pela Administração (§ 6º do art. 67 da Lei nº 14.133, de 2021).

11.3.4.4. O profissional técnico indicado poderá ocupar a posição de diretor, sócio ou integrar o quadro permanente da licitante na condição de empregado ou de prestador de serviços, devendo ser comprovada sua vinculação com a licitante, até a data da apresentação dos documentos de habilitação, por meio de carteira de trabalho e previdência social (CTPS), contrato de prestação de serviços, ficha de registro de empregado ou contrato social, conforme o caso.

11.3.4.4.1 Será admitido a apresentação de Termo de Compromisso de contratação futura assinado pela licitante e pelo profissional indicado.

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado total da contratação é de R\$ 40.000,00 (quarenta mil reais) mensais, perfazendo o valor global de R\$ 480.000,00 (quatrocentos e oitenta mil reais) para o período contratual, conforme demonstrado na tabela abaixo. Ressalta-se que o valor foi apurado a partir da Pesquisa de Preços e consolidado no respectivo Mapa Comparativo de Preços, em conformidade com o disposto no inciso XXIII, alínea "i", do art. 6º da Lei nº 14.133/2021.

ITEM 1					
SUBITEM	ESPECIFICAÇÕES	CATSER	QUANTIDADE	VALOR MENSAL	VALOR ANUAL
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	30710	12	R\$ 17.000,00	R\$ 204.000,00

2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	30736	12	R\$ 3.000,00	R\$ 36.000,00
3	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	30744	12	R\$ 8.000,00	R\$ 96.000,00
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo	30728	12	R\$ 12.000,00	R\$ 144.000,00

12.2 Para comprovar a conformidade técnica da proposta, a empresa deverá enviar no momento do envio da proposta:

- a) Documentação dos produtos ofertados: Catálogos, manuais, prospectos e outros documentos oficiais que permitam a clara identificação dos produtos. Esses documentos podem ser em português ou inglês, originais ou cópias. Não serão aceitos documentos criados especificamente para a licitação. A documentação pode ser entregue em formato eletrônico.
- b) Links de referência: Páginas da internet do fabricante do software, com indicação do endereço URL.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES.

13.2. A contratação será atendida pela seguinte dotação:

13.3. 6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

13.4. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação dos orçamentos pelo Conselho Federal de Contabilidade – CFC.

Wekson José Barbieri Mariano

Operador de Sistemas

Aprovo o Termo de Referência.

Encaminhe-se para as providências necessárias para a seleção do fornecedor, cumprindo as demais etapas legais para a contratação pública.

Contador **Walterleno Maifrede Noronha**
Presidente



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 07/10/2025, às 12:41, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 08/10/2025, às 11:07, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1055314** e o código CRC **CE436A02**.



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

TERMO Nº 90012/2025/2025/CRCES-ADM/CRCES-DIREX

Processo nº 9079618110000798.000048/2025-57

**PREGÃO
ELETRÔNICO
90012/2025**

CONTRATANTE (UASG)

Conselho Regional de Contabilidade do Espírito Santo – 383506

OBJETO

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

VALOR TOTAL DA CONTRATAÇÃO

R\$ 480.000,00

DATA DA SESSÃO PÚBLICA

Dia 29/10/2025 às 09h (horário de Brasília)

MODO DE DISPUTA:

aberto

CRITÉRIO DE JULGAMENTO:

MENOR PREÇO GLOBAL

EXCLUSIVIDADE ME/EPP/EQUIPARADAS

NÃO

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

PREGÃO ELETRÔNICO Nº 90012/2025

Processo Administrativo nº 9079618110000798.000048/2025-57

Torna-se público que o Conselho Regional de Contabilidade do Espírito Santo - CRCES, por meio do Presidente Walterleno Maifrede Noronha, sediado na rua Amélia da Cunha Ornelas, nº 30, Bento Ferreira, Vitória/ES, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da [Lei nº 14.133, de 1º de abril de 2021](#), e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

1.2. A licitação será realizada em único item.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior ensejará desclassificação no momento da habilitação, caso o cadastro no SICAF esteja desatualizado ou com incorreções, a Licitante não apresente documentação de habilitação atualizada após notificação da Pregoeira e não seja possível a verificação dos requisitos de habilitação por meio de consulta em sites oficiais.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.3. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.4. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.5. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.6. agente público do órgão ou entidade licitante;

2.6.7. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.8. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme [§ 1º do art. 9º da Lei nº 14.133, de 2021](#).

2.7. O impedimento de que trata o item 2.6.4. será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A vedação de que trata o item 2.6.8. estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.2. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.2.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.2.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do [artigo 7º, XXXIII, da Constituição](#);

3.2.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos [incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal](#);

3.2.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.3. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).

3.4. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 3º da Lei Complementar nº 123, de 2006](#), estando apto a usufruir do tratamento favorecido estabelecido em seus [arts. 42 a 49](#), observado o disposto nos [§§ 1º ao 3º do art. 4º, da Lei nº 14.133, de 2021](#).

3.4.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item.

3.4.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.5. A falsidade da declaração de que trata os itens 3.4 sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e neste Edital.

3.6. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

3.7. Não haverá ordem de classificação na etapa de apresentação da proposta, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.8. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.9. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.9.1. a aplicação do intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.9.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.10. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.10.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o

critério de julgamento por menor preço; e

3.11. O valor final mínimo parametrizado na forma do item 3.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.12. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.13. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. **preço global do item (valor anual);**

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.5.1. O prazo de validade da proposta não será inferior a **180 (cento e oitenta)** dias, a contar da data de sua apresentação.

4.6. O descumprimento das regras supramencionadas pela Administração e por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do [art. 71, inciso IX, da Constituição](#); ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo preço global do item (valor anual);

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R\$ 1.000,00 (mil reais).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Será adotado o modo de disputa “aberto”, com os licitantes apresentando lances públicos e sucessivos, com prorrogações.

5.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

5.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial, caso a contratação não se enquadre nas vedações dos §§1º e 2º do art. 4º da Lei nº 14.133, de 2021. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta forempresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123,

de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento), caso se trate de um pregão, serão consideradas empatadas com a primeira colocada.

5.18.2. A licitante mais bem classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de até 5% (cinco por cento), caso se trate de um pregão, na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.18.5. A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).

5.19.2.5. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do

primeiro colocado permanecer acima do preço máximo definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.20.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita pelo licitante, antes de findo o prazo.

5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no [art. 14 da Lei nº 14.133/2021](#), legislação correlata e no edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o [artigo 12 da Lei nº 8.429, de 1992](#).

6.3. Caso conste na Consulta de Situação do Licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. ([IN nº 3/2018, art. 29, caput](#))

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. ([IN nº 3/2018, art. 29, §1º](#)).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. ([IN nº 3/2018, art. 29, §2º](#)).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com este edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro

examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no [artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022](#).

6.7. Será desclassificada a proposta vencedora que:

- 6.7.1. conter vícios insanáveis;
- 6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;
- 6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
- 6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
- 6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

- 6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e
- 6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.10.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.11. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos [arts. 62 a 70 da Lei nº 14.133, de 2021](#).

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF, desde que os dados estejam atualizados e os documentos disponíveis para consulta.

7.2. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

7.2.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 30% (trinta por cento), para o consórcio em relação ao valor exigido para os licitantes individuais.

7.3. Os documentos exigidos para fins de habilitação poderão ser apresentados em cópia digitalizada da versão original e por documento digital-nato, declarando assim o licitante de que são legítimos e verdadeiros.

7.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei ([art. 63, I, da Lei nº 14.133/2021](#)).

7.5. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.6. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.7. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.7.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. ([IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º](#)).

7.8. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. ([IN nº 3/2018, art. 7º, caput](#)).

7.8.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. ([IN nº 3/2018, art. 7º, parágrafo único](#)).

7.9. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 02 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.10.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.11. O pregoeiro poderá realizar, de ofício, consultas junto aos sítios eletrônicos e às bases de dados estritamente oficiais, para verificação do atendimento de condições de habilitação do licitante, inclusive no tocante à documentos não apresentados.

7.11.1. Nos termos dos Acórdãos TCU nºs 1.211/2021, 2.443/2021, 2.568/2021 e 468/2022, documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta e não foi juntado com os demais comprovantes de habilitação e/ou proposta, será solicitado pelo Pregoeiro no prazo de 2 (duas) horas, sob pena de inabilitação.

7.12. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para ([Lei 14.133/21, art. 64](#), e [IN 73/2022, art. 39, §4º](#)):

7.12.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame;
e

7.12.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.13. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.14. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.15. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.16. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação ([art. 4º do Decreto nº 8.538/2015](#)).

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no [art. 165 da Lei nº 14.133, de 2021](#).

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados .

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

9.1.5. fraudar a licitação;

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação ;

9.1.8. praticar ato lesivo previsto no [art. 5º da Lei n.º 12.846, de 2013](#).

9.2. Com fulcro na [Lei nº 14.133, de 2021](#), a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e;

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato lícito, recolhida no prazo máximo de 10 (dez) dias úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato lícito.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de

15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no [art. 156, §5º, da Lei n.º 14.133/2021](#).

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do [art. 45, §4º da IN SEGES/ME n.º 73, de 2022](#).

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da [Lei nº 14.133, de 2021](#), devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, através do e-mail licitacao@crc-es.org.br.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico <https://cnc-es.org.br/>.

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I – Estudo Preliminar;

11.11.2. ANEXO II - Termo de Referência;

11.11.3. ANEXO III – Minuta de Termo de Contrato;

Vitória/ES, 13 de outubro de 2025.

Contador **WALTERLENO MAIFREDE NORONHA**
PRESIDENTE



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 13/10/2025, às 13:10, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

[https://sei.cfc.org.br/sei/controlador_externo.php?](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1063567** e o código CRC **50BE11F7**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1063567

RELAÇÃO DE ITENS - PREGÃO ELETRÔNICO Nº 90012/2025-000

1 - Itens da Licitação

1 - Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC)

Descrição Detalhada: Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço

Critério de Valor: Valor Estimado

Valor Total (R\$): 480.000,00

Unidade de Fornecimento: UNIDADE

Intervalo Mínimo entre Lances (R\$): 1.000,00

Local de Entrega (Quantidade): Vitória/ES (1)

Licitação

Dispensa/Inexigibilidade

Pedido de Cotação Eletrônica

Disponibilizar Aviso de Licitação apenas para Divulgação

11/10/2025 00:58:52



Este Aviso de Licitação será Divulgado no Portal Nacional de Contratações Públicas - PNCP e no gov.br/compras (www.gov.br/compras) na data de 14/10/2025.

Resumo do Aviso de Licitação

Órgão	UASG Responsável			
38506 - CONSELHO REGIONAL DE CONTABILIDADE/ES	383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES			
Modalidade de Licitação	Nº da Licitação	Característica	Forma de Realização	Modo de Disputa
Pregão	90012/2025	Tradicional	Eletrônico	Aberto
Lei	Critério de Julgamento			
Lei nº 14.133/2021	Menor Preço/Maior Desconto			
Tipo de Objeto				
Serviços Comuns				
Nº do Processo				
000048/2025-57				
Quantidade de Itens				
1				
Objeto				
Serviços gerenciados de Tecnologia da Informação, em Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. Gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial, conforme				
Data da Divulgação				
14/10/2025				
Data da Disponibilidade do Edital	Data/Hora da Abertura da Licitação			
A partir de 14/10/2025 às 09:00	Em 29/10/2025 às 09:00			

Disponibilizar apenas para Divulgação

Aviso de Licitação

110,00, 15 / 10006327, Sara Rodrigues Guimaraes Silva, 109,31, 16 / 10002144, Amanda Batista dos Santos, 108,40, 17 / 10001129, Juliene Vargens Ferreira, 107,86, 18 / 10004915, Fernando Jose Euzebio da Silva Melo, 102,24, 19 / 10002250, Ezequiel Felix Guimaraes, 101,83, 20 / 10004479, Everton Ferreira Teodoro, 101,64, 21 / 10006114, Barbara Dornelas dos Santos Milagres, 100,96, 22 / 10000532, Fernanda Nunes Amaral, 100,77, 23 / 10002171, Diego Henrique Guimaraes, 100,53, 24 / 10002284, Paulo Vitor Leite Braz, 99,74, 25 / 10003909, Lucas Lucio Guimaraes, 98,19, 26 / 10000914, Isabela Fernandes Xavier, 97,31, 27 / 10001712, Jonata Panza Sobrinho de Oliveira, 96,58, 28 / 10001553, Laís Loures Cruz, 96,12, 29 / 10006035, Andrey Silva Godinho, 95,93, 30 / 10000488, Clayton Matusalem da Silva, 92,65, 31 / 10006753, Poliana Silva de Melo, 92,46, 32 / 10006081, Ykaro Rodrigues Carvalho, 90,33, 33 / 10003782, Geraldo Anselmo da Silva de Andrade Melo, 90,00, 34 / 10002878, Maria Regina Novais Goncalves, 86,36, 35.

3.1.4.1 Resultado final dos candidatos negros no concurso público, na seguinte ordem: número de inscrição, nome do candidato em ordem de classificação, nota final e classificação final no concurso público.

10005670, Jessica Grazielle Pereira do Nascimento Martins, 117,93, 1 / 10000091, Sandra Suely Silva, 110,00, 2 / 10005367, Victor Hugo Gabriel Menezes Ferreira, 95,27, 3 / 10003782, Geraldo Anselmo da Silva de Andrade Melo, 90,00, 4.

3.1.5 CARGO 5: ASSISTENTE DE FISCALIZAÇÃO E ATENDIMENTO

10001537, Lucas Gandra de Moura, 182,93, 1 / 10000021, Rafael Batista Colares, 182,33, 2 / 10001035, Marcus Vinicius Santana Costa Tonaco, 169,15, 3 / 10000327, Josiel Felix de Araujo, 166,67, 4 / 10003468, Bianca Janaine Soares Cortez, 164,00, 5 / 10003531, Francielli Aparecida Borges, 160,57, 6 / 10003493, Marina Leal Barroso, 160,46, 7 / 10001334, Victor Camara Pifano Marques, 156,27, 8 / 10000205, Iara de Lima Martins, 155,93, 9 / 10005107, Arlindo Pontel da Silva, 155,33, 10 / 10004043, Gabriel Sousa de Freitas Teles, 153,67, 11 / 10005487, Thais Manhaes Alves Soares, 153,15, 12 / 10006244, Hudson Eduardo Moreira, 152,80, 13 / 10003452, Kamila Pereira de Almeida, 152,40, 14 / 10001977, Gustavo Fonseca Amaral, 151,80, 15 / 10006267, Izabela Silva Bueno, 151,70, 16 / 10006126, Mireille Cassia Fonseca Reis, 151,22, 17 / 10003105, Julia Padovezi Miranda, 151,17, 18 / 10000285, Renault Fernandes Ferreira Junior, 150,72, 19 / 10000381, Daysiane Rocha Souza, 150,53, 20 / 10005414, Nicole Carrilho Knopp Alves, 150,22, 21 / 10003181, Felipe Couto de Oliveira Araujo, 150,10, 22 / 10006164, Fabiano Carlos Santana e Silva, 149,43, 23 / 10002431, Marla Oliveira Souza, 148,57, 24 / 10003483, Alexia de Souza Lima Assis, 147,71, 25 / 10005442, Ariel Batista Aguiar, 147,35, 26 / 10004754, Kalida Karielle do Nascimento Amaral, 145,98, 27 / 10004980, Thayane Iolanda Dias Almeida, 143,27, 28 / 10003673, Leticia Janine Ferreira Faria, 140,40, 29 / 10001074, Lucas de Souza Marinho, 140,33, 30 / 10004471, Luis Gustavo Cunha da Fonseca, 140,17, 31 / 10002310, Gustavo Alves Ribeiro**, 138,29, 32 / 10002408, Mariana Godinho Ferreira Costa, 138,24, 33 / 10001266, Bryan Junio Goncalves Pereira, 137,40, 34 / 10006058, Clarissa Martins de Vasconcelos, 136,29, 35 / 10004380, Carolina Franco Leal, 136,00, 36 / 10000256, Carlos Filipe Lopes Gomes da Silva, 135,73, 37 / 10004507, Fabio Cezar Rodrigues de Deus, 135,60, 38 / 10002474, Samara Lopes, 135,27, 39 / 10002843, Paloma Messias Goncalves, 134,73, 40 / 10005703, Guilherme Mello Guimaraes de Carvalho, 134,60, 41 / 10005396, Patricia Aparecida de Oliveira, 133,83, 42 / 10003616, Marcello Teixeira Monnerat, 133,50, 43 / 10003896, Clarisse Maria da Silva, 133,41, 44 / 10006667, Ana Rayssa Saraiva Basilio, 133,00, 45 / 10000520, Junio Jose Borges Barbosa, 132,81, 46 / 10005197, Carolina de Souza Lima, 132,10, 47 / 10000632, Tayna Emilli Rosa e Pereira, 132,10, 48 / 10005667, Rafael Henriques da Silva, 131,57, 49 / 10004360, Roger Drumond Fernandes, 131,21, 50 / 10005572, Marcelo de Castro e Souza, 129,98, 51 / 10006073, Claudia Ferreira de Almeida, 129,96, 52 / 10006646, Mateus Campos Rodrigues, 129,69, 53 / 10002509, Jurrain Dias Menezes, 128,60, 54 / 10002106, Caio Marcio Lopes Goncalves, 127,73, 55 / 10005283, Henrique Jose Nogueira Pereira, 127,23, 56 / 10005571, Josiane de Souza Mendes, 127,21, 57 / 10006680, Monique Moreira Borges, 127,20, 58 / 10005206, Matheus Filipe Toshy Dozono, 125,96, 59 / 10003584, Hugo Deleon Souza, 125,83, 60 / 10004660, Lucas de Freitas Melo, 123,71, 61 / 10002735, Rafael Frasson Cecato Cabral, 123,02, 62 / 10000088, Flavio Reis Ferreira e Silva*, 120,87, 63 / 10005274, Wallisson Augusto Soares de Carvalho, 119,37, 64 / 10006098, Sara Fernanda Pinheiro Barcelos*, 106,50, 65.

3.1.5.1 Resultado final dos candidatos negros no concurso público, na seguinte ordem: número de inscrição, nome do candidato em ordem de classificação, nota final e classificação final no concurso público.

10004043, Gabriel Sousa de Freitas Teles, 153,67, 1 / 10006244, Hudson Eduardo Moreira, 152,80, 2 / 10002474, Samara Lopes, 135,27, 3 / 10002843, Paloma Messias Goncalves, 134,73, 4 / 10006667, Ana Rayssa Saraiva Basilio, 133,00, 5 / 10004086, Adenilson Ferreira de Souza, 130,93, 6 / 10002509, Jurrain Dias Menezes, 128,60, 7 / 10005571, Josiane de Souza Mendes, 127,21, 8 / 10000952, Jhonatan Pereira Dornelas Borges, 124,33, 9 / 10004627, Mario Henrique da Silva Santos, 122,67, 10 / 10000463, Iuri Ferreira Pimenta, 121,53, 11 / 10006650, Elaine Cristine Santos Santana, 120,27, 12 / 10000308, Welberth Quirino dos Santos, 115,67, 13 / 10004909, Jhonatan Vieira Barbosa, 114,10, 14 / 10001722, Fabio Jesus de Souza Figueiredo, 112,86, 15 / 10006257, Juliana Rodrigues Soares, 110,38, 16 / 10004515, Alcimar Andrade Barcelos, 109,00, 17 / 10005991, Lucas Luciano Bambirra e Silva, 105,74, 18 / 10003145, Josiane dos Santos de Jesus, 102,33, 19 / 10003712, Laís Tereza dos Santos Souza, 101,86, 20 / 10000792, Pedro Silva Machado, 98,94, 21 / 10002538, Nicibel Edvania da Silva, 95,13, 22 / 10006168, Mateus Henrique da Silva Ferreira, 94,60, 23 / 10000029, Paulo Cesar Dias, 91,67, 24.

(*) Candidatos considerados pessoas com deficiência na avaliação biopsicossocial, aprovados somente como pessoas com deficiência.

(**) Candidatos considerados pessoas com deficiência na avaliação biopsicossocial, aprovados em ampla concorrência e como pessoas com deficiência.

(1) Candidatos negros que obtiveram pontuação suficiente para aprovação em ampla concorrência dentro do número de vagas por cargo.

4 DAS DISPOSIÇÕES FINAIS

4.1 As justificativas da banca para o deferimento ou indeferimento dos recursos interpostos contra o resultado provisório na avaliação biopsicossocial dos candidatos que solicitaram concorrer às vagas reservadas às pessoas com deficiência e no resultado provisório do procedimento de heteroidentificação dos candidatos que se autodeclararam negros estarão à disposição dos candidatos a partir da data provável de 17 de outubro de 2025, no endereço eletrônico http://www.cebraspe.org.br/concursos/cau_mg_25.

4.1.1 O Cebraspe não arcará com prejuízos advindos de problemas de ordem técnica dos computadores, de falhas de comunicação, de congestionamento das linhas de comunicação e de outros fatores, de responsabilidade do candidato, que impossibilitem a visualização das justificativas da banca para o deferimento ou indeferimento.

4.2 O resultado final no concurso público fica devidamente homologado nesta data pela Presidente do CAU/MG.

CECÍLIA FRAGA DE MORAES GALVANI

CONSELHO DE ARQUITETURA E URBANISMO DO RIO GRANDE DO SUL

EXTRATO DE TERMO DE ADITIVO

Extrato: 4º Termo de Aditivo ao Contrato nº 027/2021. Processo Administrativo: 119/2020. Modalidade: Pregão Eletrônico. Objeto: Serviços Contínuos de Limpeza, manutenção e conservação e copeiragem com dedicação exclusiva de mão de obra. Contratante: Conselho de Arquitetura e Urbanismo do Rio Grande do Sul - CAU/RS, CNPJ 14.840.270/0001-15; Contratado: PARANA LIMP SERVIÇOS TERCEIRIZADOS EIRELI, CNPJ: 06.059.231/0001-57. Prazo de Vigência: 27/12/2025 a 27/12/2026; Cobertura Orçamentária: 6.2.2.1.01.04.04.012 - Serviços de Reparos, Adapt. e Conserv. de Bens Móveis e Imóveis. Data de Assinatura: 06/10/2025. Signatários: pelo CAU/RS, Andrea Hamilton Ilha, Presidente do CAU/RS, e pelo contratado, Claudineia Pereira, Diretora.

CONSELHO FEDERAL DE MEDICINA

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 90022/2025 - UASG 925158

Nº Processo: 25.0.000007684-0.

Objeto: Contratação de empresa especializada para a prestação de serviços para a execução de MANUTENÇÃO PREVENTIVA E CORRETIVA nos elevadores instalados na sede do Conselho Federal de Medicina - CFM, em Brasília/DF, com fornecimento de peças originais, mão de obra qualificada, suporte técnico e atendimento emergencial, visando garantir o pleno funcionamento, segurança e durabilidade dos equipamentos, de 06 (seis) elevadores da marca KONE, a serem executados de forma contínua para atender a sede do Conselho Federal de Medicina, conforme as características, condições, obrigações e requisitos contidos no termo de referência e demais anexos. Total de Itens Licitados: 1. Edital: 14/10/2025 das 08h00 às 12h00 e das 13h00 às 17h00. Endereço: SGAS, Qd. 616 Conjunto D, lote 115, L2 Sul - Bairro Asa Sul - Brasília/DF ou <https://www.gov.br/compras/edital/925158-5-90022-2025>. Entrega das Propostas: a partir de 14/10/2025 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 29/10/2025 às 10h30 no site www.gov.br/compras. Informações Gerais: Em caso de discordância existente entre as especificações deste objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

ANTONIO CESAR NEVES FRANCISCO
Pregoeiro

CONSELHO FEDERAL DE QUÍMICA

EXTRATO DO CONVÊNIO Nº 41/2025

Partes: Conselho Federal de Química - CFQ e Conselho Regional de Química da 8ª Região - CRQ VIII.

Objeto: doação no valor de R\$ 73.600,00 (setenta e três mil e seiscentos reais) destinado ao Projeto de Fiscalização 2025 do Conveniente.

Vigência: 03/10/2025 a 03/10/2026.

Assinam:

Rildo Araújo Laytynher, Presidente do CRQ VIII
José de Ribamar Oliveira Filho, Presidente do CFQ

EXTRATO DE TERMO ADITIVO

3º TERMO ADITIVO

Processo SEI nº 2800.00.02319.2025 - Termo de Contrato nº 12/2022 - Contratante: Conselho Federal de Química. Contratada: Lavanderia Cristal Serviços Expressos Eireli ME. (CNPJ 01.319.181/0001-86). Objeto: prorrogação do prazo contratual por 12 (doze) meses e reajuste de preços da prestação de serviço de limpeza e higienização das toalhas de mesa. Vigência: 05/10/2025 a 04/10/2026. Data da assinatura: 02/10/2025. Valor R\$ 6.127,04. Base legal: Parágrafo único do art. 61 da Lei nº 8.666, de 1993.

CONSELHO REGIONAL DE ADMINISTRAÇÃO DA BAHIA

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 90.005/2025

UASG 389136 Nº Processo: 476901003044/2025-44.

A presente licitação tem por objeto a contratação de empresa operadora de plano de saúde coletivo empresarial para prestação de serviços de assistência médico-hospitalar, hospitalar com obstetrícia, ambulatorial e laboratorial para realização de procedimentos clínicos, cirúrgicos e obstétricos, atendimento de urgência e emergência, exames complementares, serviços auxiliares de diagnóstico, procedimentos terapêuticos e internações, sem exclusão de doenças e lesões preexistentes ou crônicas, através de plano de saúde, de acordo com a Lei Federal nº 9.656 de 03/06/1998 e suas regulamentações, com cobertura em todo o território nacional, com acomodação em apartamento, para atendimento aos funcionários do CRA-BA, sendo extensivo a seus dependentes., de acordo com o Termo de Referência deste Pregão Eletrônico nº 90.005/2025. Endereço atual do CRA-BA: Av. Tancredo Neves, 999, Edifício Metropolitan Alfa, sala 602, Caminho Das Árvores - Salvador/BA com divulgação, no D.O.U., no gov.br/compra, no PNCP (Portal Nacional de Contratações Públicas) e no site do CRA-BA: www.cra-ba.org.br. Entrega das Propostas: a partir de 14/10/2025 às 08h00, no site www.gov.br/compras. Abertura das Propostas 29/10/2025 às 10h:00 no site www.gov.br/compras. Adm. MARIO AUGUSTO BEHRENS FREIRE - Pregoeiro CRA-BA.

MARIO AUGUSTO BEHRENS FREIRE

CONSELHO REGIONAL DE ADMINISTRAÇÃO DA PARAÍBA

AVISO DE DISPENSA DE LICITAÇÃO

COMPRAS Nº 25/2025-CRA-PB/CONTRATAÇÃO POR DISPENSA DE LICITAÇÃO

O Conselho Regional de Administração da Paraíba- CRA-PB, torna público a necessidade de aquisição de material/serviços conforme Termo de Referência nº 80/2025) disponível em <https://cra.pb.implanta.net.br/portalttransparencia/#publico/Lista?id=fa3b82be-fb73-4ea5-9941-ed23402276a3> Os interessados devem enviar proposta para compras2@crapb.org.br com o título : Proposta referente ao Processo SEI nº 476912.001124/2025-36 Objeto: Contratação de assessoria e acompanhamento técnico em comemoração a Profissão de administração. Prazo para envio de proposta 72h, a contar da data de publicação do aviso (14.10.2025), Prazo de recebimento da proposta: 72h - 16.10.2025 - ATÉ AS 14HS

João Pessoa 13 de outubro de 2025.
MARIA VERÔNICA SILVA DOS SANTOS
Agente de Contratação

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

AVISOS DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 90012/2025 - UASG 383506

PREGÃO ELETRÔNICO Nº 90012/2025 - Objeto: Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, notebooks, servidores e monitores, tudo em conformidade com as condições, quantidades e exigências estabelecidas no Edital e seus anexos. Total de Itens: 1. Edital disponível: <https://crc-es.org.br/novas-licitacoes> e <https://www.gov.br/compras>. Entrega das Propostas: a partir de 14/10/2025 às 09h00 no site www.gov.br/compras. Abertura das Propostas: 29/10/2025 às 09 horas no site www.gov.br/compras. Informações Gerais: licitacao@crc-es.org.br.

PREGÃO ELETRÔNICO Nº 90013/2025

PREGÃO ELETRÔNICO Nº 90013/2025 - Objeto: Contratação de empresa especializada para: (1) desenvolvimento completo de um novo portal institucional web para o Conselho Regional de Contabilidade do Espírito Santo (CRC-ES), contemplando arquitetura moderna, responsiva e acessível, desenvolvido com tecnologias atuais de mercado; (2) prestação de serviços de manutenção do portal web pelo período de 12



(doze) meses; e (3) prestação de serviços de hospedagem do portal web pelo período de 12 (doze) meses, conforme condições e exigências estabelecidas no Edital e seus anexos. Total de Itens: 1. Edital disponível: <https://crc-es.org.br/novas-licitacoes> e <https://www.gov.br/compras>. Entrega das Propostas: a partir de 14/10/2025 às 09h00 no site www.gov.br/compras. Abertura das Propostas: 30/10/2025 às 09 horas no site www.gov.br/compras. Informações Gerais: licitacao@crc-es.org.br.

PREGÃO ELETRÔNICO Nº 90014/2025

PREGÃO ELETRÔNICO Nº 90014/2025 - Objeto: Aquisição de assinatura do Microsoft 365 Business standard, com chat, chamada e conferência de vídeo com o Microsoft Teams pelo período de 12 (doze) meses), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos. Total de Itens: 1. Edital disponível: <https://crc-es.org.br/novas-licitacoes> e <https://www.gov.br/compras>. Entrega das Propostas: a partir de 14/10/2025 às 09h00 no site www.gov.br/compras. Abertura das Propostas: 31/10/2025 às 09 horas no site www.gov.br/compras. Informações Gerais: licitacao@crc-es.org.br.

Em 8 de outubro de 2025
WALTERLEO MAIFREDE NORONHA
Presidente

CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DO AMAPÁ**EXTRATO DE CONTRATO**

ESPECIE: TERMO DE CONTRATO. Oriundo da Inexigibilidade de licitação nº. 907606110000201.000052/2025-70. Contratante: CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DO AMAPÁ e a Contratada: TVLANDIA EMPREENDIMENTOS IMOBILIÁRIOS LTDA, inscrita no CNPJ nº 05.043.280/0001-39. OBJETO: Locação de espaço de eventos para atender às demandas decorrentes da realização do XIV Fórum da Mulher Contabilista do Amapá, a ser realizada nos dias 10 e 11 de outubro de 2025. VIGÊNCIA: 02 (dois) dias. DOTAÇÃO ORÇAMENTÁRIA: 6.3.1.3.02.01.027 - Locação de bens móveis. VALOR: R\$ 20.000,00 (vinte mil reais).

CONSELHO REGIONAL DE CONTABILIDADE DE RONDÔNIA**EXTRATO DE TERMO ADITIVO**

Terceiro Termo Aditivo ao Contrato nº 011/2022, referente ao Processo nº 9079610110000359.000046/2023-08. Contratada: G3 COMERCIO E SERVIÇOS LTDA - CNPJ: 11.757.232/0001-05. Objeto: Prorrogar o prazo de vigência, suprimir a franquia atual e reajustar o valor nos termos do Contrato nº 011/2022, tendo a redução de 5.000 páginas por mês para 4.000 páginas mês, e aplicar o reajuste que corresponde o percentual de 5,1 % pela variação do IPCA. Vigência: 11/10/2025 a 10/10/2026. Dispositivo Legal: Art.65, I, alínea b, §§ 1º e 2º, da Lei nº 8.666/93. Data da Assinatura: 08/10/2025.

CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DA 15ª REGIÃO**EDITAL DE NOTIFICAÇÃO**

O Presidente do Conselho Regional de Corretores de Imóveis 15ª. Região/CE, no uso das atribuições legais que lhe foram conferidas, e em conformidade com o disposto nos artigos 47 e seguintes da Resolução - COFECI nº 146/82; depois de esgotadas as tentativas de ciência por meio de notificação via remessa postal e através da fiscalização da entidade, NOTIFICAR as partes interessadas do inteiro teor da decisão adotada na Sessão da Primeira Turma Julgadora deste Conselho, ocorrida em 27 de março de 2025, referente ao processo administrativo disciplinar n.º 2023.15.20096283 que consta como Representada: AIRTON FERNANDES CONSULTORIA IMOBILIÁRIA LTDA, CRECI Nº 8.939; e Representante: JOANEMILY MARIA RIBEIRO ALVES: "DECISÃO DA 1ª. TURMA JULGADORA DO CRECI/CE: A Primeira Turma Julgadora do Conselho Regional de Corretores de Imóveis 15ª. Região/CE, designada pela Portaria - CRECI nº 005/2025, reunida no auditório da MRH em Fortaleza, situado na Rua Professor Jacinto Botelho, nº 1600 (Térreo) - Bairro Guararapes, na Sessão de Julgamento realizada em 27 de março de 2025, apreciando o Processo de Representação nº. 2023.15.20096283 DECIDIU, através de votação nominal, por unanimidade, aprovar o voto do relator, pela PROCEDÊNCIA da Representação e pela aplicação da pena de CANCELAMENTO DA INSCRIÇÃO com a respectiva apreensão do Certificado de Inscrição da pessoa jurídica representada, cumulada com a pena de MULTA equivalente a 03(três) anuidades. Sessão presidida pelo Coordenador da 1ª. Turma Julgadora do CRECI-15ª. Região/CE, Conselheiro LUIZ ANDRÉ MOURÃO MELO, e secretariada pelo Conselheiro ÁULIO FAÇANHA ANTUNES." De acordo com a legislação em vigor, a contar do recebimento do presente ofício, V.Sa. tem o prazo de 30 (trinta) dias para, querendo, apresentar recurso junto ao COFECI - Conselho Federal de Corretores de Imóveis, na forma do artigo 53 do Código de Processo Disciplinar (Resolução - COFECI nº 146/82).

Fortaleza (CE), 16 de junho de 2025.
TIBÉRIO VITORIANO BENEVIDES DE MAGALHÃES

**AVISO DE SUSPENSÃO
PREGÃO ELETRÔNICO Nº 7/2025**

Nº Processo Administrativo: 2025.15.30122749

CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DO CEARÁ - CRECI/CE 15ª REGIÃO, Por intermédio de sua Pregoeira Márcia Fernanda Muxió dos Santos Alves, comunica aos interessados no PREGÃO ELETRÔNICO Nº 07/2025 a SUSPENSÃO do certame com abertura marcada para às 10h horas do dia 15/10/2025, em razão de revisão e retificação do Termo de Referência e Edital, cujo objeto é a contratação de empresa especializada para fornecimento de solução tecnológica de comunicação corporativa baseada em PABX Virtual (Chatbot), com Contact Center Omnichannel integrado ao WhatsApp Business API Oficial, conforme as especificações detalhadas no Termo de Referência. Face o exposto, oportunamente, será publicada nova data de abertura da licitação pela mesma via em que se deu a publicação original. Fortaleza/CE, 10 de outubro de 2025. MÁRCIA FERNANDA MUXÍO DOS SANTOS ALVES - Pregoeira.

Fortaleza-CE, 10 de outubro de 2025.
MÁRCIA FERNANDA MUXÍO DOS SANTOS ALVES
Pregoeira

CONSELHO REGIONAL DE EDUCAÇÃO FÍSICA DA 14ª REGIÃO**AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 90005/2025 - UASG 926461**

Torna-se público que o Conselho Regional de Educação Física da 14ª Região CREF14/GO-TO, por meio do seu presidente, realizará Pregão Eletrônico, referente a Aquisição de 25 tablets para o CREF14, com critério de julgamento MENOR PREÇO, na hipótese do nos termos do art.28, I e art.29, da Lei Federal nº 14.133, de 01 de Abril de 2021. Data da sessão: 28/10/2025 às 09 horas. Link: <https://www.gov.br/compras/pt-br>

MARCELO DE CASTRO SPADA RIBEIRO
Presidente

CONSELHO REGIONAL DE EDUCAÇÃO FÍSICA DA 15ª REGIÃO**AVISO DE DISPENSA DE LICITAÇÃO ELETRÔNICA Nº 13/2025
PROCESSO ADMINISTRATIVO Nº 13/2025**

DISPENSA DE LICITAÇÃO ELETRÔNICA Nº 13/2025 - CREF15/PI

OBJETO: FORMAÇÃO DE REGISTRO DE PREÇOS para eventual contratação de empresa especializada em SERVIÇOS DE AGENCIAMENTO DE VIAGENS, compreendendo a cotação, reserva, emissão, marcação, remarcação e cancelamento de bilhetes de passagens aéreas, em trechos nacionais, para atender às demandas do Conselho Regional de Educação Física (CREF15). VALOR TOTAL ESTIMADO PARA O REGISTRO: R\$ 45.794,28 (quarenta e cinco mil, setecentos e noventa e quatro reais e vinte e oito centavos) Tipo: Dispensa Eletrônica CRITÉRIO DE JULGAMENTO: Maior desconto percentual

MODO DE DISPUTA: Aberto PARTICIPAÇÃO EXCLUSIVA ME/EPP/EQUIPARADAS: Não.

ÓRGÃO REALIZADOR: CONSELHO REGIONAL DE EDUCAÇÃO FÍSICA DA 15ª REGIÃO (CREF15/PI) - UASG: 926885.
ENDEREÇO: Rua Primeiro de Maio, nº 2024, Marquês, Teresina/PI, CEP 64.002-510. SÍLIO ELETRÔNICO: www.cref15.org.br.

HORÁRIO DE FUNCIONAMENTO: Das 08h00m às 16h59m (Horário local). DATA DA REALIZAÇÃO DA SESSÃO PÚBLICA: 17/10/2025.

HORÁRIO DA FASE DE LANCES: Das 09h às 15h (Horário de Brasília). ENDEREÇO ELETRÔNICO (LINK DE ACESSO): <https://www.gov.br/compras/pt-br>

AGENTE DE CONTRATAÇÃO: Aline da Silva Oliveira.
APOIO: Willany Felix da Silva.

(Portaria - Presidência Nº 15/2025 - CREF15/PI, 02 de dezembro de 2024). TELEFONE: (86) 3085-2182 - E-MAIL: cpl@cref15.org.br.

LEGISLAÇÃO APLICÁVEL: Leis Nacionais / Federais: Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos), Lei Complementar nº 123/2006 (Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte), Lei nº 8.078/1990 (Código de Defesa do Consumidor) e demais leis aplicáveis ao objeto. Instruções Normativas Federais: Instrução Normativa SEGES/ME nº 67/2021 (Dispõe sobre a dispensa de licitação, na forma eletrônica), Decreto nº 11.462/2023 (Dispõe sobre o sistema de registro de preços para a contratação de bens e serviços, no âmbito da Administração Pública federal direta, autárquica e fundacional), Instrução Normativa SEGES/MPDG nº 3/2018 (Estabelece regras de funcionamento do Sistema de Cadastro Unificado de Fornecedores - SICAF)..

Teresina-PI, Em 13 de outubro de 2025.
DANYS MARQUES MAIA QUEIROZ
Presidente CREF15

CONSELHO REGIONAL DE EDUCAÇÃO FÍSICA DA 9ª REGIÃO**EDITAL DE NOTIFICAÇÃO**

INSCRIÇÃO EM DÍVIDA ATIVA

O CONSELHO REGIONAL DE EDUCAÇÃO FÍSICA DA 9ª REGIÃO - ESTADO DO PARANÁ - CREF9/PR, no uso de suas atribuições legais vem NOTIFICAR, na forma o art. 201 do CTN, Lei Federal nº 6.830/80, Lei Federal nº 9696/1998, Lei Federal nº 12.514/2011, Lei Federal nº 11.000/2004, Decreto Federal nº 70.235/1972 e demais Resoluções do Sistema CONFEF/CREFs, as pessoas físicas/jurídicas abaixo relacionadas, para que impreterivelmente, até 30 (trinta) dias, contados dessa publicação, compareçam na sede desta autarquia, no endereço, Rua Doutor Faivre, nº 880, Centro, Curitiba/PR, ou contate pelo telefone (41) 3363-8388, a fim de pagar, parcelar ou apresentar defesa relativa aos débitos apurados, sob pena de inscrição de dívida ativa e posterior protesto em cartório ou ajuizamento de execução fiscal. A presente notificação refere-se apenas aos débitos de anuidades/multas do período de 2020 a 2024. Constituem o rol dos notificados os seguintes registros profissionais de pessoa física e registros de pessoa jurídica: PR-033393 SIMONE PEREIRA DA FONSECA, PR-034208 GISELAINE CRISTINA KOHUT, PR-035501 ALLAN ELIAKIM DE SOUSA FERREIRA, PR-035507 LUCAS MATHEUS DE SOUZA RODRIGUES, PR-038124 SANDRO ROBERTO DE GODOY, PR-038552 EDUARDO ALEXANDRE GONÇALVES DE ARAUJO, PR-038801 GUSTAVO RIBEIRO CAETANO, PR-039676 GUILHERME GOMES FERREIRA, PR-034287 GEISA ADRIANA VENDRAMETTO, PR-035549 MONICA DE SOUZA CARVALHO LOPES, PR-035185 DANILO DOS SANTOS BUENO, PR-039583 KECIELLY ANDRADE CANO, PR-036880 JESSICA DE JESUS SCALADA, PR-038771 ANDREA DE FATIMA DA ROSA SCREMIN, PR-039120 TAMIRES FERNANDA FERREIRA, PR-037960 GEISIANE RAFAELA CRESCENCIO DE MELO BIAGGIO, PR-039705 FABIO DE SOUZA GONÇALVES, PR-034682 ANDRE LUIS TOLEDO DE BORBA, PR-037313 AMANDA BENATO PAMPUCHE, PR-034728 RAFAEL BUBNIAK, PR-037508 NATÁ GUILHERME TRENTINI, PR-038025 RODRIGO DE FREITAS GRITZ, PR-033500 JOSIEL DIAS, PR-035363 DANIELLE DAYANE FIORERIZ DE MITO TARTARELLI, PR-038950 LUCAS DA SILVA MORAES, PR-033122 ELITON SIQUEIRA LOPES, PR-033492 ESTEFANIA SILVA DOS SANTOS, PR-035169 DIESLEY DE PAULA MAINARDES, PR-033266 FRANKLIN DA LUZ, PR-034349 WILMA DA COSTA MEDEIROS, PR-034556 JOAO PEDRO FOIATTO DOS SANTOS, PR-034766 KAMILA CRISTINA CEZARI, PR-034813 ROBSON ANDRE CORREIA, PR-035583 HILLARY DE SOUZA ALVES, PR-035586 ROBSON AMORIM FERREIRA, PR-036135 MARLON RIBEIRO SEBAGE, PR-036347 LUCAS HENRIQUE MARTINS COSTA, PR-036480 LEONARDO DONADI MESSIAS, PR-035638 ROBSON DIEGO FERREIRA LARA, PR-037043 JOSE HENRIQUE BLAHUM FONSECA, PR-037048 LUIS ANTONIO SOARES DE SOUZA, PR-037954 SERGIO PEREIRA BARBOSA, PR-038665 RAFAELA APARECIDA BELOTTO DE SOUZA, PR-039169 EDVALDO ALVES DE SOUZA, PR-033264 FABRICIO LINS VELOSO, PR-033638 HENRIQUE SOUZA DA SILVA, PR-035413 JONATAS RODRIGUES BASTOS, PR-035808 THIAGO HENRIQUE SILVA, PR-036751 REINALDO JUNIOR ZAFALON, PR-037454 MAICON JUNIOR PEREIRA, PR-034691 ELOIR JUNIOR DA SILVA DOS SANTOS, PR-036341 ALLYSON PEDROSO, PR-034733 VIVIANA MARIA BAMPÁ MUNHOZ, PR-038475 KELEN GARCIA MASHNI, PR-039774 FERNANDO HENRICH PEREIRA, PR-033205 RAFAEL GARCIA CRUZ, PR-033212 THALIA YOHANA SAMPAIO, PR-033402 MARIANA DE OLIVEIRA DE SOUZA, PR-033483 SONIA MARA DE CARVALHO RIBEIRO D. NUNES, PR-033631 AURILENO MOREIRA BERNARDI, PR-033726 ELISÂNGELA ALVES TEIXEIRA, PR-033979 TIAGO DE MIRANDA VIEIRA, PR-034268 DAVID SOUZA DE SABOYA BARBOSA, PR-034270 BRUNA DOS SANTOS PIMENTEL, PR-034277 JORGE PAULO GOMES DA SILVA JUNIOR, PR-034351 FABIO RENATO MENDONÇA SALGADO FILHO, PR-034374 LETÍCIA MARTINS DA SILVA, PR-034385 MICHELLY MARCONDES, PR-034447 DOUGLAS PEREIRA NUNES, PR-033491 KARINE FERNANDA VIEIRA ALVES, PR-034917 YURI SOARES DA SILVA, PR-035066 JEFFERSON PEREIRA DE ALMEIDA, PR-035115 MATHEUS RICARDO CORREA GIUSTI, PR-035119 MONIQUE DE PAULA DE BRITO DE LIMA, PR-035138 RAWLINS RAY CESAR GONZALEZ DAU, PR-035165 HERLON LINS CALDAS, PR-035219 YAN ALVES RIBAS, PR-035470 ALLAN GUIMARÃES ROSA, PR-035479 DAIANA ANGELA BARBOSA, PR-035568 MARINA FANHA CRUZ, PR-035686 ARTHUR BARCELOS XAVIER, PR-035716 JESSICA FRANCO VIEIRA PRENDIN, PR-035724 JOELMA TEIXEIRA DE ALMEIDA PATRICIO DE JESUS, PR-035764 CECILIA ESPERANÇA GALETTO, PR-035904 GABRIEL ROMANELLI RODRIGUES, PR-035919 RODOLFO ALBERTO MARRIQUE BENITO, PR-035975 STELLA REGINA RICARDO PRADO CORREA, PR-036042 NIEGGE SUZANNE TAVARES, PR-036181 LUCAS MATHEUS DOS SANTOS, PR-036220 WAGNER ALEX SANDRO DA SILVA, PR-036277 BRUNA BENTO DOS SANTOS, PR-036401 MARCIO MARIA ANTUNES RAMOS, PR-036534 THIAGO WILLIAM CORRÊA DOS SANTOS, PR-036610 MAISA APARECIDA MARCAL, PR-036664 MARCO AURELIO CARVALHO GOMES, PR-036668 SUELEN COSTA MALDONADO MIRANDA CAETANO, PR-036694 MELISSA ALVES CORREA, PR-036727 PRISCILA VIEIRA LOPES, PR-036837 PAOLA NAICILLI GONÇALVES, PR-036841 RODRIGO DE OLIVEIRA DUNAISKI, PR-036876 PATRICIA ALICE NUNES DA SILVA, PR-037095 RAFAEL FONSECA NASCIMENTO, PR-037231 FREDERICO DE SOUZA AMELO, PR-037520 ROGER DOS SANTOS PEREIRA, PR-037807 LEVI BEZERRA DA CONCEIÇÃO, PR-037852 ARLINDO JOSE DOS SANTOS FILHO, PR-038024 JOSUÉ PEREIRA REIS, PR-038095 IGOR DIAS ALVES, PR-038176 MARCIA CRISTINA CABRAL DA ROSA, PR-038212 THIAGO CARDOSO MARTINS, PR-038220 JEAN ANDREY ALMEIDA BITENCOURT, PR-038318 DOUGLAS FELIPE DE SOUZA BREVES, PR-038606 LUCAS SIQUEIRA FRANCA RIBEIRO, PR-038686 DANIELA MARIA DA SILVA MEDEIROS, PR-038949 FAUZI ZAKI KATZER TADROS, PR-038956 ALESSANDRA DA SILVA ARECO GOIS, PR-038958 DANIEL HENRIQUE CARON WEISS, PR-039062 MARCOS EDUARDO MANENTE CHELLA, PR-039396 MARCELO ANDRADE DE LIMA, PR-039563 MARIANA OLIVEIRA GUIMARÃES, PR-037206 VALDEMIR LEMES, PR-039664 EVELIN KESIANE ALAMINI, PR-039420



Edital nº 90012/2025

[Acessar Contratação](#)

Última atualização 14/10/2025

Local: Vitória/ES **Órgão:** CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

Unidade compradora: 383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES

Modalidade da contratação: Pregão - Eletrônico **Amparo legal:** Lei 14.133/2021, Art. 28, I **Tipo:** Edital

Modo de disputa: Aberto **Registro de preço:** Não **Fonte orçamentária:** Não informada

Data de divulgação no PNCP: 14/10/2025 **Situação:** Divulgada no PNCP

Data de início de recebimento de propostas: 14/10/2025 09:00 (horário de Brasília)

Data fim de recebimento de propostas: 29/10/2025 09:00 (horário de Brasília)

Id contratação PNCP: 28163343000196-1-000052/2025 **Fonte:** Compras.gov.br

Objeto:

Serviços gerenciados de Tecnologia da Informação, em Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. Gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial, conforme detalhamento no Edital e anexos.

Informação complementar:

Para as respostas de esclarecimentos e impugnações deste edital acesse o link:
<https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/landing?destino=quadro-informativo&compra=38350605900122025>

VALOR TOTAL ESTIMADO DA COMPRA

R\$ 480.000,00

[Itens](#)

[Arquivos](#)

[Histórico](#)

Número	Descrição	Quantidade	Valor unitário estimado	Valor total estimado
1	Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC)	1	R\$ 480.000,00	R\$ 480.000,00

Exibir: 5

1-1 de 1 itens

Página:

1



[< Voltar](#)



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.

É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e corretude das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portaldeservicos.gestao.gov.br>

☎ [0800 978 9001](tel:08009789001)

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à **licença de uso**.

PUBLICAÇÃO LEGAL

EDITAIS • COMUNICADOS • BALANÇOS • CONVENÇÕES • PRESTAÇÕES DE CONTAS



TERÇA-FEIRA, 14 DE OUTUBRO DE 2025 » WWW.ESHOJE.COM.BR » BIANCA@ESHOJE.COM.BR » ANUNCIE: (27) 2180-0678 PAG.1

COMUNICADO
"CASA DAS TELHAS E MAD. LTDA" torna público que **OBTEVE** da **SEMMA**, **LMAR 109/25**, para desenvolvimento da atividade "**Serraria e/ou fabricação de artefatos (...)**", **cód 8.01**, na localidade de **R. Curio, 11, Pontal da Garças, Vila Velha**.

COMUNICADO
CARLOS JOSE FILHO 78069190744, CNPJ nº 41.133.432/0001-58, torna público que **requereu**, por meio do processo nº **107251/2025** à **PMVV/SEMMA**, **LMAR-S** para desenvolvimento da atividade de **Triagem, lavagem, processamento, beneficiamento e/ou armazenamento temporário de resíduos sólidos reutilizáveis e/ou recicláveis não perigosos e não contaminados com óleos e graxas minerais, agrotóxicos ou produtos químicos**, cuja titularidade não seja de Associação de Catadores ou entidade equivalente, respeitado o ente responsável pelo licenciamento da Central de Tratamento de Resíduos quando associado a uma (cód. 20.02) - Classe S, na Rua Maria do Nascimento Pereira, nº 36, Primeiro de Maio, Vila Velha/ES.

COMUNICADO
A DA FAZENDA COMERCIO LTDA, inscrita no CNPJ 50.441.581/0001-75, localizada na **Avenida Central, Nº 13, Nova Bethânia, - Viana/ES**, torna público que **obteve** da Secretaria Municipal de Meio Ambiente de Viana, através do processo nº **21160/2024**, a Licença Municipal de Regularização, para a atividade **Estocagem, armazenamento ou depósito exclusivo para grãos e outros produtos alimentícios, (associado ou não à classificação rebeneficiamento)**, incluindo **frigoríficos (Não Industrial)** na localidade **Avenida Central nº 100, Galpão 2, Bairro Campo Verde, Viana-ES**.

COMUNICADO
FELIPE DE SOUZA DE CASTRO - Pousada Praia LTDA CNPJ 44.051.325/0001-79 torna público que **requereu** a **SEMA Guarapari ES** através do processo nº **27307/2025 - LAR**, para atividade de **Hotelaria**, na **Av. Praiana, nº 427, Praia do Morro, 29.216-090, Guarapari/ES**.

COMUNICADO
"EUROTEXTIL COM. E IMP. LTDA" torna público que **requereu** da **SEMMA**, através do Proc. **111994/25**, a **LMAR/S**, para "**Estocagem, armazenamento (...)**", **cód 22.09**, na localidade de **R. Darcy D. Carneiro, 20, Rod. Daryl Santos, 800, Galpão 01 - Áreas 1A a 1C, Jardim Asteca, Vila Velha, 29.104-491**.

COMUNICADO
NOVAMED ENXOVAIS CORPORATIVOS E COMERCIO LTDA, CNPJ nº 15.344.568/0001-05, torna público que **requereu**, por meio do processo nº **112607/2025**, à **PMVV/SEMMA**, **LMAR-S** para desenvolvimento da atividade **estocagem, armazenamento ou depósito para cargas gerais, exclusivamente em galpão fechado (cód. 22.09)**, à **Rua Adao Jacinto, s/nº, Quadra 02, Lotes 04-A, 06, 07 e 08, Divino Espírito Santo, Vila Velha/ES**.

COMUNICADO
"AUTO POSTO SCHUENG XXII LTDA", torna público que **OBTEVE** da **SEMDEC**, através do processo nº **9905/2025**, Licença **LID nº 14/2025**, para a atividade de **Posto Revendedor de Combustíveis sem atividade de lavagem de veículos e troca de óleo**, na localidade de **Morada de Santa Fé** no Município de **Cariacica**.

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 038/2025
Proc. Nº 32.236/2024
Objeto: Provável aquisição de Uniformes, para atender a Secretaria de Serviços - SEMSERV, no Município de Cariacica/ES
Recebimento das propostas: de 15/10/2025 a 29/10/2025, às 13:30 h. Abertura das propostas e sessão de Disputa: 29/10/2025 às 14:00 h. Edital disponível nos sites www.portaldecompraspublicas.com.br, www.cariacica.es.gov.br e www.gov.br/pncp/pt-br. Maiores informações poderão ser obtidas através do telefone: (27) 3354-5815. E-mail: pregao5@cariacica.es.gov.br ID.TCE/ES: 2025.017E0600015.01.0004
Cariacica-ES, 13/10/2025
IASCARA BEZERRA DE MENEZES
Agente de Contratação

AVISO DE ABERTURA
PREGÃO ELETRÔNICO
N 000049/2025 (SRP)
WCompras ID 429294
CÓDIGO CIDADES : 2025.072E0700001.01.0032
A Prefeitura Municipal de Venda Nova do Imigrante, através da Equipe de Pregão, torna pública a realização de certame licitatório, conforme segue: Pregão Eletrônico nº 000049/2025 WCompras ID 429294. Objeto **CONTRATAÇÃO DOS SERVIÇOS DE FORNECIMENTO, APLICAÇÃO E BOMBAMENTO DE CONCRETO USINADO FKC 30MPA**. Acolhimento das propostas a partir do dia: 15/10/2025 às 08:00h. Limite de acolhimento de propostas: 30/10/2025 às 08h30 min. Início da sessão de disputa: 30/10/2025 às 09:00h. Edital disponível nos sites www.portaldecompraspublicas.com.br e www.vendanova.es.gov.br
Alexandra de Oliveira Vinco
Pregoeira Oficial

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 023/2025
Proc. Nº 31.963/2025
Objeto: Registro de Preços para provável aquisição de materiais médicos hospitalares. Recebimento das propostas: de 15/10/2025 a 29/10/2025, às 10:00h. Abertura das propostas e sessão de Disputa: 29/10/2025 às 10h15min. Critério de julgamento: menor preço global. Modo de disputa: aberto e fechado. Legislação aplicável: 14.133/2021. Órgão requisitante: Secretaria Municipal de Saúde. Edital disponível nos sites: www.cariacica.es.gov.br e www.gov.br/pncp/pt-br www.portaldecompraspublicas.com.br Maiores informações poderão ser obtidas através do telefone: (27) 3354-5815. E-mail: pregao2@cariacica.es.gov.br ID.Cidades: 2025.017E0500002.01.0018
Cariacica-ES, 13/10/2025.
VANIA APARECIDA GANHO
Agente Contratação

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 90014/2025 -
Objeto: Aquisição de assinatura do Microsoft 365 Business standard, com chat, chamada e conferência de vídeo com o Microsoft Teams pelo período de 12 (doze) meses), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos. Total de Itens: 1. Edital disponível: <https://crc-es.org.br/novas-licitacoes> e <https://www.gov.br/compras>. Entrega das Propostas: a partir de 14/10/2025 às 09h00 no site www.gov.br/compras. Abertura das Propostas: 31/10/2025 às 09 horas no site www.gov.br/compras. Informações Gerais: licitacao@crc-es.org.br.
WALTERLENO MAIFREDE NORONHA
Presidente

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 036/2025
Proc. Nº 31.950/2025
Objeto: Registro de Preços para provável aquisição de fralda descartável infantil (produto de higiene pessoal), atender a Secretaria de Saúde - SEMUS. Recebimento das propostas: de 15/10/2025 a 28/10/2025, às 14:00h. Abertura das propostas e sessão de Disputa: 28/10/2025 às 14h15min. Critério de julgamento: menor preço global. Modo de disputa: aberto e fechado. Legislação aplicável: 14.133/2021. Órgão requisitante: Secretaria Municipal de Saúde. Edital disponível nos sites: www.cariacica.es.gov.br e www.gov.br/pncp/pt-br www.portaldecompraspublicas.com.br Maiores informações poderão ser obtidas através do telefone: (27) 3354-5815. E-mail: pregao2@cariacica.es.gov.br ID.Cidades: 2025.017E0500002.01.0020
Cariacica-ES, 13/10/2025.
VANIA APARECIDA GANHO
Agente Contratação

AVISO DA LICITAÇÃO
Pregão Eletrônico
nº 90008/2025
Órgão: Secretaria Estadual das Mulheres - SESM
UASG: 930251
Processo: 2025-8D2KZ
ID C I D A D E S : 2025.500E0600027.01.0010
Objeto: SERVIÇOS CONTINUADOS DE LIMPEZA, HIGIENIZAÇÃO, COPELAGEM E RECEPÇÃO COM A DISPONIBILIZAÇÃO DE MÃO-DE-OBRA, FORNECIMENTO DE MATERIAIS, EQUIPAMENTOS, FERRAMENTAS E UTENSÍLIOS, necessários à execução dos serviços, para atendimento às necessidades da SECRETARIA ESTADUAL DAS MULHERES. Valor total estimado: R\$ 4.065.917,40. Início da Sessão Pública: 30/10/2025 às 14h. O certame será realizado por meio do Sistema Compras do Governo Federal (www.gov.br/compras), estando o edital disponível no Portal Nacional de Contratações Públicas (PNCP) e endereço: www.compras.es.gov.br. Os interessados em participar da licitação deverão efetuar seu cadastro no Sistema de Cadastro Unificado de Fornecedores - SICAF e no sistema de compras do Governo Federal. Contato: licitacao@mulheres.es.gov.br
ROBERTA DA SILVA ABREU
Agente de Contratação - SESM

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 019/2025
PROCESSO Nº 4547/2025
CÓDIGO CIDADES TCE/ES Nº 2025.052E0700001.01.0025
Objeto: Contratação de empresa especializada na execução de serviços de transporte escolar, sob a forma de fretamento, para atendimento aos alunos do ensino infantil, ensino fundamental, educação de jovens e adultos (EJA) e ensino médio do município de Nova Venécia-ES, adeso ao Programa Estadual de Transporte Escolar - PETE/ES - LINHAS ESTADUAIS E COMPARTILHADAS. Local: Bolsa de Licitações do Brasil - BLL - <https://bllcompras.com/Home/Login> Data de abertura: 29/10/2025. Horário máximo de recebimento da proposta: 08h30min (Horário de Brasília-DF). Horário do início da disputa: 09h00min (Horário de Brasília-DF). O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.bll.org.br e www.novavenecia.es.gov.br, e também poderá ser lido e/ou obtido através do e-mail licitacao@novavenecia.es.gov.br ou no endereço da Prefeitura Municipal de Nova Venécia/ES, situada na Avenida Vitória, nº 347, Centro, Nova Venécia/ES, CEP: 29.830-000, nos dias úteis, no horário de 08h00min às 11h00min e das 13h00min às 17h00min. Informações pelo tel. (27) 3752-9004. Nova Venécia/ES, 13/10/2025
RÔMULO DELBONI DOS SANTOS
SECRETÁRIO MUNICIPAL DE EDUCAÇÃO

Acesse o www.eshoje.com.br e ouça a nossa Rádio Web

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 002/2025
PROCESSO Nº 2910/2025
CÓDIGO CIDADES TCE/ES Nº 2025.052E0500002.01.0002
Objeto: Aquisição de enxoval para recém-nascido, para suprir as necessidades da Secretaria Municipal de Assistência Social dentro do Programa de Concessão de Benefícios Eventuais - Auxílio-natalidade. Local: Bolsa de Licitações do Brasil - BLL - <https://bllcompras.com/Home/Login> Data de abertura: 27/10/2025. Horário máximo de recebimento da proposta: 08h00min (Horário de Brasília-DF). Horário do início da disputa: 08h30min (Horário de Brasília-DF). O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.bll.org.br e www.novavenecia.es.gov.br, e também poderá ser lido e/ou obtido através do e-mail licitacao@novavenecia.es.gov.br ou no endereço da Prefeitura Municipal de Nova Venécia/ES, situada na Avenida Vitória, nº 347, Centro, Nova Venécia/ES, CEP: 29.830-000, nos dias úteis, no horário de 08h00min às 11h00min e das 13h00min às 17h00min. Informações pelo tel. (27) 3752-9004. Nova Venécia/ES, 13/10/2025
RÔMULO DA SILVA BAIA
SECRETÁRIO MUNICIPAL DE ASSISTÊNCIA SOCIAL

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO
Nº 90012/2025 -
Objeto: Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores, tudo em conformidade com as condições, quantidades e exigências estabelecidas no Edital e seus anexos. Total de Itens: 1. Edital disponível: <https://crc-es.org.br/novas-licitacoes> e <https://www.gov.br/compras>. Entrega das Propostas: a partir de 14/10/2025 às 09h00 no site www.gov.br/compras. Abertura das Propostas: 29/10/2025 às 09 horas no site www.gov.br/compras. Informações Gerais: licitacao@crc-es.org.br.
WALTERLENO MAIFREDE NORONHA
Presidente





(<https://crc-es.org.br>)

  / @sigacrces  / CRCES TV



(<https://www3.cfc.org.br/spw/PortalTransparencia/Consulta.aspx?CS=qFg6mE2Yq8U=>)

procurar no site

Menu Principal



Selecione a Modalidade:

Todas ▼

Buscar por Processo CRC-ES nº

90012/2025

Selecione a Situação:

Todas ▼

Período

até



Privacidade - Termos

Localizar

Total de resultados: 2

	Processo CRC-ES nº	Situação	Modalidade	Nº/Ano	Data de Abertura	Objeto da Contratação



	PREGÃO ELETRÔNICO Nº 90012/2025	Em Andamento	Pregão Eletrônico	90012/2025	29/10/2025	Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e 

						corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

Hora Abertura	Valor	CNPJ Fornecedor	Nome Fornecedor
09:00	-	-	-

Arquivos para Download

Edital 90012.2025 GERENCIAMENTO DE TI (<https://crc-es.org.br/wp-content/uploads/2025/10/Edital-90012.2025-GERENCIAMENTO-DE-TI.zip>)



Q	Aviso de Contratação Direta nº 90012/2025	Anulada	Dispensa de licitação	12/2025	08/05/2025	Contratação de empresa para atuar como agente integrador, responsável pelo preenchimento de vagas de menor aprendiz e estágio supervisionado a estudantes regularmente matriculados e com frequência efetiva em instituições de ensino médio, técnico ou superior, destinadas às atender às necessidades do CRCES, conforme detalhamento, quantitativo e especificações contidas no Termo de Referência – anexo do Aviso de Contratação Direta.



dade-Do-
ES/346581458693:

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

Rua Amélia da Cunha Ornelas, 30 - Bento Ferreira - Vitória - ES - CEP: 29050-620 - Tel: (27) 3232-1600

O atendimento presencial será às segundas, quartas e sextas das 13 às 16h,
devendo o mesmo ser por agendamento

Copyright © 2025 CRC - ES , todos os direitos reservados





Selecção de fornecedores - Julgamento

Online

Pregão Eletrônico N° 90012/2025 (Lei 14.133/2021)

UASG 383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES ?

Critério julgamento: Menor Preço / Maior Desconto Modo disputa: Aberto



Disputa



Julgamento



Habilitação



Fase Recursal



Adjudicação/ Homologação



1 SERVIÇOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA D...
Aguardando julgamento

Qtde solicitada: 1
Valor estimado (unitário) R\$ 480.000.0000



44.447.862/0001-32 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 289.000,0000 Valor negociado (unitário) -	REDES VIX LTDA ES	▼
48.431.950/0001-05 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 292.000,0000 Valor negociado (unitário) -	GABRIEL ALEX RAMIRO MARTINS 22834623805 SP	▼
70.946.330/0001-50 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 293.000,0000 Valor negociado (unitário) -	INFRA DO BRASIL COMERCIO E SERVICOS LTDA MG	▼
52.851.499/0001-44 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 304.000,0000 Valor negociado (unitário) -	WINK TELECOMUNICACOES LTDA AM	▼
55.298.629/0001-51 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 310.000,0000 Valor negociado (unitário) -	SMART FUSION TECHNOLOGY LTDA ES	▼
14.698.571/0001-56 Programa de integridade Valor ofertado (unitário) R\$ 340.000,0000 Valor negociado (unitário) -	AT&TI SOLUCOES EM TECNOLOGIA LTDA ES	▼
15.549.061/0001-80 Programa de integridade Valor ofertado (unitário) R\$ 383.000,0000 Valor negociado (unitário) -	PRINT SOLUCAO EM TECNOLOGIA LTDA ES	▼
23.936.997/0001-91 Programa de integridade	MGDATA TECNOLOGIA LTDA MG	



37.007.414/0001-52 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 390.000,0000 Valor negociado (unitário) -	INFINITY STORE COMERCIO E SERVICOS DE INFORMATICA LTDA RO	▼
29.297.426/0001-30 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 460.000,0000 Valor negociado (unitário) -	INFOMAX SOLUCOES EM TECNOLOGIA LTDA SE	▼
57.135.675/0001-65 ME/EPP Valor ofertado (unitário) R\$ 464.000,0000 Valor negociado (unitário) -	COMERCIAL LENA LTDA SP	▼
10.215.066/0001-52 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 465.000,0000 Valor negociado (unitário) -	FUTURA SOLUCOES NETWORKS E SERVICOS LTDA MG	▼
10.635.032/0001-17 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 475.000,0000 Valor negociado (unitário) -	MECSAM SERVICOS DE ENGENHARIA LTDA AM	▼
32.586.528/0001-80 ME/EPP Programa de integridade Valor ofertado (unitário) R\$ 480.000,0000 Valor negociado (unitário) -	MA TECNOLOGIA LTDA ES	▼
36.770.097/0001-69 Programa de integridade Valor ofertado (unitário) R\$ 495.456,0000 Valor negociado (unitário) -	CIB EMPREENDIMENTOS IMOBILIARIOS LTDA MG	▼
10.757.593/0001-99 Programa de integridade Valor ofertado (unitário) R\$ 1.480.000,0000 Valor negociado (unitário) -	THS TECNOLOGIA INFORMACAO E COMUNICACAO LTDA DF	▼

[Voltar](#)[Anular](#)[Revogar](#)

**ILUSTRÍSSIMO(A) SENHOR(A) PREGOEIRO(A) DO CONSELHO REGIONAL DE CONTABILIDADE DO
ESPÍRITO SANTO – CRC ES – REFERENTE AO PREGÃO ELETRÔNICO Nº 90012/2025**

A **PRINT SOLUÇÃO EM TECNOLOGIA LTDA**, sociedade empresária por cotas de responsabilidade limitada, inscrita no CNPJ sob o n.º 15.549.061/0001-80, com sede na cidade de Vila Velha, Estado do Espírito Santo, na Rua Maranhão, 575 - Salas 501 a 504 - Ed. Torre Sul, Praia da Costa - CEP n.º 29.101-340, por seu representante legal infra-assinado – de agora em diante mencionada apenas por **RECORRENTE** – vem, na forma do disposto no item do Edital e legislação complementar, apresentar as **RAZÕES DE RECURSO** contra a decisão que resolveu por desclassificar a **PRINT SOLUÇÃO EM TECNOLOGIA LTDA** e classificar, habilitar e declarar vencedora a proposta da Empresa **REDES VIX LTDA** para o ITEM 1 do referido processo licitatório, doravante designada **RECORRIDA** ou **REDES VIX**, com fulcro nos fatos e argumentos a seguir anotados.

DA TEMPESTIVIDADE DO RECURSO

Tendo tomado ciência do conteúdo da proposta da **RECORRIDA**, da declaração de vencedora para o **ITEM 01** do referido certame, a **RECORRENTE** manifestou intenção de recurso, conforme orientação do próprio edital.

Portanto, é tempestivo o presente recurso e merece ser conhecido.

DOS MOTIVOS PARA DESCLASSIFICAÇÃO DA PROPOSTA DA EMPRESA RECORRIDA

A seguir apresentamos as razões de recurso, devidamente enumeradas, as quais revistos os documentos apresentados e anexados à proposta da **RECORRIDA**, evidencia-se o equívoco do julgador, visto estarem infringidos requisitos exigidos no instrumento convocatório. Além disso, ressaltaremos a falha no julgamento de alguns pontos.

RAZÃO I

O não atendimento técnico de diversos pontos do edital.

Devido a licitante não ter atendido vários pontos do edital com os equipamentos fornecidos e para facilitar a análise desses pontos montamos uma tabela onde referência os pontos do edital e as problemáticas causadas pelo não atendimento.

Equipamentos ofertados pela licitante:

“U7 Pro Max”

“S6500-24GP4XF”

“FortiGate 80F”

Print Solução em Tecnologia Ltda

 +55 27 3063-6663  27 999795-8588

 print@printsolucao.com.br

 www.printsolucao.com.br

Segue tabela de não atendimento dos itens ofertados:

Item do TR	Descrição
2.5.1.1	Configuração 100% centralizada em controlador
	Sem esse recurso, cada AP pode exigir configuração individual ou parcialmente distribuída, isso gera: maior tempo de implantação, risco de configurações divergentes entre APs, necessidade de administrar APs um a um.
2.5.1.2	Compatível/gerenciado pelo NGFW do termo
	O firewall não consegue ver, controlar ou aplicar políticas diretamente nos APs. Consequências: perda de visibilidade de aplicações por SSID, impossibilidade de aplicar políticas de segurança centralizadas, não existe coordenação entre firewall e rede wireless.
2.5.1.3	Operação obrigatoriamente centralizada (AP dependente)
	Sem essa função, o AP não depende totalmente do controlador, podendo operar de forma independente. Isso afeta: recursos de segurança centralizada, funções de túnel, políticas unificadas.
2.5.1.4	Descoberta automática do controlador
	Sem descoberta automática, cada AP teria que ser apontado manualmente para o controlador. Impactos: aumento do tempo de provisionamento, maior risco de erro humano;
2.5.1.8	Rádio dedicado para WIDS/WIPS
	Sem rádio dedicado, o AP precisa usar o mesmo rádio de acesso para “escutar” ataques. Consequências: queda de desempenho do WiFi, proteção contra intrusão menos eficaz, não garante detecção contínua 24/7.
2.5.1.11	1GbE + 2.5GbE (duas portas)
	Sem portas multigig + porta redundante: limita throughput real do AP (especialmente WiFi 6/7), não permite uplink redundante, reduz desempenho agregado quando muitos clientes conectam
2.5.1.13	Link Aggregation 802.3ad
	Sem agregação de link: não é possível somar portas para aumentar banda, não há redundância de uplink no AP, impossibilita operação de failover L2.
2.5.1.14	Porta console RS-232/USB
	Sem porta console: impossibilidade de recuperação local via CLI caso perca o acesso de rede, dificulta troubleshooting em ambientes críticos, aumenta tempo de reparo.
2.5.1.15	Entrada 12VDC + PoE Injector incluso
	Sem alimentação alternativa: não funciona sem PoE no switch, limita flexibilidade de instalação.
2.5.1.16	Encaminhamento centralizado via túnel AP→controlador
	Sem túnel central: tráfego sai direto pelo AP, sem ir ao controlador, perde inspeção centralizada, não permite políticas unificadas entre filiais.
2.5.1.17	Túnel IPSec AP→controlador
	Sem IPSec: tráfego entre AP e controlador pode ir sem criptografia forte, não atende cenários WAN seguras entre prédios/unidades.

Print Solução em Tecnologia Ltda

+55 27 3063-6663 27 999795-8588

print@printsolucao.com.br

www.printsolucao.com.br

2.5.1.18	Split tunneling configurado no SSID
Sem split tunneling: todo tráfego vai pelo mesmo caminho, não é possível separar tráfego local x corporativo, pode causar sobrecarga no controlador ou firewall.	
2.5.1.34	Identificação automática de interferências (2.4/5GHz)
Sem isso: o AP não identifica canais poluídos automaticamente, pior experiência de cliente, necessidade de tuning manual constante.	
2.5.1.35	Análise de espectro para interferências não-WiFi
Sem análise de espectro: o AP não detecta micro-ondas, bluetooth, câmeras sem fio, etc., troubleshooting de interferência exige ferramentas externas, degradações invisíveis ficam difíceis de resolver.	
2.5.1.38	Até 14 SSIDs simultâneos
Se o AP suporta menos SSIDs: não atende a estrutura exigida (rede visitante, IoT, voz, dados, etc.), limita segmentação da rede WiFi.	
2.5.1.41	802.1X com VLAN dinâmica via atributos RADIUS
Sem isso: não é possível colocar automaticamente cada usuário em uma VLAN específica, segurança reduzida, impossibilita segregação por função/departamento.	
2.5.1.42	Métodos EAP avançados (AKA, SIM, FAST, TTLS)
Sem suporte: incompatibilidade com ambientes corporativos que usam EAP avançado, pode impedir autenticação WiFi de smartphones corporativos ou gov.	
2.5.1.49	Gerenciamento via SNMP
Sem SNMP: ferramentas de monitoramento como Zabbix/Nagios/SolarWinds não conseguem coletar métricas, reduz visibilidade operacional, não permite alertas automáticos.	
2.5.1.50	REST API diretamente no AP
Sem API: impossibilita automação e integrações modernas, dependência somente do controlador, reduz capacidade de gestão via scripts ou sistemas externos.	
2.6.1.7	Taxa de encaminhamento requerida (190 Mpps) e switch entrega ~95.2 Mpps
Em ambientes de alto tráfego: o switch pode saturar, queda de performance, aumento de latência, risco de perda de pacotes.	
2.6.1.10	Latência $\leq 1 \mu s$ não especificada pelo fabricante
Sem garantia de latência: desempenho pode variar, sensível para VoIP, vídeo e aplicações em tempo real, degrada a qualidade do WiFi backhaul.	
2.6.1.18	IGMP Snooping com 1000 entradas não comprovado na documentação
Sem tabela IGMP grande: IPTV ou multicast corporativo podem falhar, excessivo broadcast multicast, degrada a rede WiFi quando usa multicast-to-unicast.	
2.6.1.32-40	Funcionalidades avançadas de 802.1X/MAB/CoA/Guest VLAN/Autenticação múltipla não confirmadas
Sem esses recursos: autenticação de usuários na borda fica limitada, não é possível múltiplos dispositivos na mesma porta (telefone + PC), CoA não funciona → políticas RADIUS não atualizam dinamicamente, não atende requisitos de segurança Zero Trust, dificulta uso de VLAN dinâmica de voz/dados.	

2.6.1.44-46	Controle de MAC por porta, aging customizado e logs avançados não documentados
Sem esses mecanismos: não é possível identificar mudanças suspeitas de MAC, mais difícil detectar ataques ARP spoofing e MAC move, troubleshooting manual se torna mais complexo.	
2.6.1.56	Deteção de conflito de IP e envio de trap SNMP não documentado
Sem essa capacidade: conflitos IP não são detectados automaticamente, a rede pode apresentar quedas intermitentes difíceis de diagnosticar, não há geração de alertas automáticos via NMS.	

Justificativa da razão: Fica claro que a licitante não tem expertise para entregar a solução ofertada e entregou equipamentos totalmente divergentes do solicitado.

DO CUMPRIMENTO A NORMAS E CONDIÇÕES DO EDITAL PELA ADMINISTRAÇÃO PÚBLICA

No ato convocatório constam todas as normas e critérios aplicáveis à licitação. É por meio dele que o Poder Público chama os potenciais interessados em contratar com ele e apresenta o objeto a ser licitado, o procedimento adotado, as condições de realização da licitação, bem como a forma de participação dos licitantes. Nele devem constar necessariamente os critérios de aceitabilidade e julgamento das propostas, bem como as formas de execução do futuro contrato.

Conforme deliberação do TCU, como por exemplo, no Acórdão 3474/2006 - Primeira Câmara, onde os ministros acordaram que: “O edital é a lei interna do processo de licitação, vinculando aos seus termos tanto a Administração Pública como os licitantes. Não seria aceitável que a Administração fixasse no edital a forma e o modo de participação dos licitantes e, no decorrer do processo ou na realização do julgamento, se afastasse do estabelecido. Ou ainda, que aceitasse de apenas um dos participantes a apresentação de proposta em desacordo com o estabelecido”.

CONSIDERAÇÕES FINAIS

Destaca-se ainda que o julgamento de qualquer proposta para um processo licitatório deve se apoiar em fatores concretos, pedidos pela Administração, em confronto com o ofertado pelos licitantes, dentro dos parâmetros fixados no edital.

“O princípio do julgamento objetivo afasta a discricionariedade na escolha das propostas, obrigando a Comissão de Julgamento a se ater ao critério prefixado pela Administração, levando sempre em consideração o interesse do serviço público. No julgamento das propostas, a Comissão levará em consideração os critérios objetivos definidos no Edital.” (Marçal Justen Filho - 2005)
Vale lembrar a jurisprudência do TCU sobre o tema, tal como:

Jurisprudência do TCU:

“A decisão subjetiva é rechaçada pelo ordenamento jurídico, que impõe o julgamento objetivo e a vinculação ao edital, em homenagem aos princípios constitucionais da isonomia, da impessoalidade e da moralidade.

Como se observa, a legalidade e a vinculação ao ato convocatório são manifestações jurídicas de

Print Solução em Tecnologia Ltda

 +55 27 3063-6663  27 999795-8588

 print@printsolucao.com.br

 www.printsolucao.com.br

princípios inter-relacionados. A validade dos atos administrativos praticados no curso da licitação depende de sua compatibilidade não apenas com a Lei, mas também com os atos administrativos praticados nas etapas anteriores.

DO PEDIDO

Em face dos argumentos ora apresentados, enfatizando a obrigatoriedade de atendimento aos princípios administrativos basilares de toda e qualquer licitação, e ainda, com base na demonstração inequívoca do não atendimento a requisitos técnicos por parte da proposta da empresa **REDES VIX LTDA**, requer a **RECORRENTE**:

- a) Que a decisão que declarou a proposta vencedora seja revogada e a proposta da empresa **REDES VIX** seja desclassificada;
- c) Que o certame seja retomado, examinando a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que atenda integralmente a este edital;
- d) Que caso a Comissão não entenda assim, que o processo seja encaminhado a Autoridade Superior para apreciação;

Confia a **PRINT SOLUÇÃO EM TECNOLOGIA LTDA** no senso de justiça dessa Comissão de Licitação, na capacitação técnica da equipe que a assessora, para o restabelecimento da verdade dos fatos.

Nestes Termos
Pede e Espera Deferimento

Vila Velha (ES), 01 de dezembro de 2025

A handwritten signature in black ink, appearing to read "Walter Maia Rodrigues Júnior", is written over a light blue rectangular background.

Walter Maia Rodrigues Júnior

Diretor Comercial

RG: [REDACTED]

CPF: [REDACTED]

Print Solução em Tecnologia Ltda

+55 27 3063-6663 27 999795-8588

print@printsolucao.com.br

www.printsolucao.com.br

CONTRARRAZÕES DE RECURSO ADMINISTRATIVO

PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 90012/2025.

CONTRATANTE: CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO – CRCES.

RECORRENTE: PRINT SOLUÇÃO EM TECNOLOGIA LTDA.

RECORRIDA: REDES VIX LTDA.

Assunto: Impugnação às Razões de Recurso apresentadas pela empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA.

1. INTRODUÇÃO

A empresa REDES VIX LTDA, devidamente qualificada e declarada vencedora do ITEM 1 do Pregão Eletrônico nº 90012/2025, vem, respeitosamente, apresentar suas contrarrazões ao Recurso Administrativo interposto pela empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA.

O recurso da PRINT se baseia em uma interpretação restritiva e descontextualizada do Termo de Referência (TR), ignorando a natureza da solução proposta pela REDES VIX, que atende integralmente aos requisitos funcionais e de desempenho exigidos, muitas vezes superando-os, por meio de uma arquitetura moderna e integrada.

A seguir, refutamos ponto a ponto as alegações de não atendimento técnico, demonstrando a plena conformidade da proposta da REDES VIX com o edital, em estrito cumprimento ao princípio do julgamento objetivo.

2. DA PLENA CONFORMIDADE TÉCNICA DA PROPOSTA DA REDES VIX

A PRINT SOLUÇÃO EM TECNOLOGIA LTDA fundamenta seu recurso na alegação de que os equipamentos ofertados pela REDES VIX — notadamente o Access Point "U7 Pro Max", o Switch "S6500-24GP4XF" (TP-Link Omada Pro) e o Firewall "FortiGate 80F" — não cumprem diversos itens do Termo de Referência.

A análise da PRINT é falha por quatro motivos principais:

- 1 Confusão entre Requisito Funcional e Solução Específica:** O TR estabelece requisitos funcionais (o que a solução deve fazer), e não impõe uma arquitetura de fabricante específica. A solução da REDES VIX, composta por equipamentos Ubiquiti UniFi e Fortinet, atende aos requisitos através de sua gestão centralizada e software de controle.
- 2 Desconhecimento da Integração da Solução:** A PRINT analisa os equipamentos de forma isolada, ignorando a integração entre o NGFW (FortiGate) e o Switch (S6500-24GP4XF), bem como a

gestão centralizada do Wi-Fi via software controlador (UniFi Network Application) e a gestão do switch via Omada SDN Controller, que é a solução viável e permitida pelo TR.

- 3 **Interpretação Excessivamente Literal:** Em diversos pontos, a PRINT exige características que não são mandatórias ou que são atendidas por equivalência tecnológica superior.
- 4 **Interesse Comercial na Venda de Solução Integrada de Alto Custo:** A análise técnica da PRINT demonstra um interesse comercial subjacente em promover sua própria solução integrada. Ao exigir características muito específicas e analisar a concorrência de forma isolada e literal, a PRINT busca desclassificar soluções viáveis e mais econômicas, como a proposta pela REDES VIX. O objetivo é forçar a adoção de um pacote de equipamentos e serviços, muitas vezes de um único fabricante, com valores inflacionados e margens de lucro elevadas. Esse aumento artificial dos custos do projeto não é do interesse público, pois resulta em um desperdício de recursos e uma contratação excessivamente onerosa para a administração.

A tabela a seguir refuta cada uma das alegações apresentadas pela Recorrente, demonstrando a conformidade da proposta da REDES VIX.

Item do TR	Alegação da PRINT (Não Atendimento)	Justificativa e Solução Viável (REDES VIX)
2.5.1.1	Configuração 100% centralizada em controlador.	ATENDE. A linha UniFi (U7 Pro Max) é controller-based. A configuração, monitoramento e gestão são 100% centralizados através do UniFi Network Application (software controlador), que pode ser instalado em um servidor local ou em nuvem, conforme a arquitetura proposta. O AP não opera sem o controlador.
2.5.1.2	Compatível/gerenciado pelo NGFW do termo.	ATENDE VIA INTEGRAÇÃO. O TR não exige que o NGFW (FortiGate 80F) seja o controlador de APs. A gestão de segurança e políticas é feita pelo FortiGate, enquanto a gestão do Wi-Fi é feita pelo controlador UniFi. A solução atende ao requisito de segurança (NGFW) e gestão de rede (Controlador UniFi), cumprindo o objetivo funcional do TR.
2.5.1.3	Operação obrigatoriamente centralizada (AP dependente).	ATENDE. Os APs UniFi são dependentes do controlador para configuração e monitoramento avançado. Embora possam continuar transmitindo em caso de falha do controlador (modo standalone), a gestão e as políticas de segurança são centralizadas, cumprindo o requisito de operação centralizada.
2.5.1.4	Descoberta automática do controlador.	ATENDE. Os APs UniFi utilizam mecanismos de descoberta automática (Layer 2 e Layer 3, via DHCP Option 43 ou DNS), facilitando o provisionamento e reduzindo o risco de erro humano, conforme exigido.
2.5.1.8	Rádio dedicado para wIDS/wIPS.	ATENDE POR EQUIVALÊNCIA. O U7 Pro Max possui um rádio dedicado para segurança (wIDS/wIPS) e análise de espectro, além dos rádios de 2.4GHz, 5GHz e 6GHz. A alegação da PRINT é factualmente incorreta.

Item do TR	Alegação da PRINT (Não Atendimento)	Justificativa e Solução Viável (REDES VIX)
2.5.1.11	1GbE + 2.5GbE (duas portas).	ATENDE POR EQUIVALÊNCIA SUPERIOR. O U7 Pro Max possui uma porta 2.5GbE e uma porta 1GbE (PoE-in), totalizando duas portas, sendo uma delas Multi-Gigabit, o que é superior ao requisito mínimo de 1GbE + 2.5GbE, garantindo o throughput necessário para o Wi-Fi 7.
2.5.1.13	Link Aggregation 802.3ad.	ATENDE. O U7 Pro Max suporta Link Aggregation (LAG), permitindo somar as portas 2.5GbE e 1GbE para aumentar a banda e fornecer redundância de uplink, conforme o padrão 802.3ad.
2.5.1.14	Porta console RS-232/USB.	SOLUÇÃO VIÁVEL. Embora o AP UniFi não possua porta console física tradicional, o acesso de recuperação é feito via SSH ou através do controlador centralizado. Para troubleshooting local, o acesso via SSH pela rede é o padrão de mercado para equipamentos modernos, sendo uma solução viável e mais eficiente.
2.5.1.15	Entrada 12VDC + PoE Injector incluso.	ATENDE POR EQUIVALÊNCIA. O U7 Pro Max é alimentado por PoE++ (802.3bt), que é o padrão de alimentação mais robusto e seguro para APs de alto desempenho. A alimentação 12VDC é uma alternativa menos comum em ambientes corporativos. O switch S6500-24GP4XF (PoE+ 802.3at) fornece a alimentação via PoE, garantindo a alimentação. A alimentação 12VDC é uma alternativa menos comum em ambientes corporativos, e a oferta de PoE+ atende ao requisito funcional de alimentação.
2.5.1.16	Encaminhamento centralizado via túnel AP→controlador.	ATENDE POR EQUIVALÊNCIA. O UniFi opera em modo Local Bridging, onde o tráfego de dados é encaminhado diretamente para a rede local (LAN), enquanto o tráfego de gestão é encapsulado. O TR não exige o encapsulamento de dados para o controlador, apenas a gestão centralizada. A arquitetura de Local Bridging é a mais eficiente para evitar sobrecarga no controlador/firewall.
2.5.1.17	Túnel IPSec AP→controlador.	ATENDE POR EQUIVALÊNCIA. O tráfego de gestão entre o AP e o controlador UniFi é criptografado. Para cenários WAN seguras, o FortiGate 80F é o equipamento responsável por estabelecer túneis IPSec entre unidades, cumprindo o requisito de segurança de WAN.
2.5.1.18	Split tunneling configurado no SSID.	ATENDE. O controlador UniFi permite a configuração de VLANs e regras de firewall (ACLs) por SSID, possibilitando o Split Tunneling para separar tráfego local (LAN) de tráfego corporativo (VPN/WAN), atendendo ao requisito funcional.

Item do TR	Alegação da PRINT (Não Atendimento)	Justificativa e Solução Viável (REDES VIX)
2.5.1.34	Identificação automática de interferências (2.4/5GHz).	ATENDE. O UniFi Network Application possui recursos avançados de Channel Optimization e RF Scan que identificam automaticamente interferências e otimizam os canais, melhorando a experiência do cliente.
2.5.1.35	Análise de espectro para interferências não-WiFi.	ATENDE. O U7 Pro Max, com seu rádio de segurança dedicado, realiza Análise de Espectro para detectar fontes de interferência não-WiFi (micro-ondas, Bluetooth, etc.), facilitando o troubleshooting e a otimização da rede.
2.5.1.38	Até 14 SSIDs simultâneos.	ATENDE. Os APs UniFi suportam o número de SSIDs exigido pelo TR, permitindo a segmentação completa da rede (Visitante, IoT, Voz, Dados, etc.).
2.5.1.41	802.1X com VLAN dinâmica via atributos RADIUS.	ATENDE. O UniFi Network Application suporta autenticação 802.1X e VLAN Dinâmica através de atributos RADIUS (VLAN ID, Tunnel-Private-Group-ID), permitindo a segregação de usuários por função/departamento.
2.5.1.42	Métodos EAP avançados (AKA, SIM, FAST, TTLS).	ATENDE. O UniFi suporta os principais métodos EAP, incluindo EAP-TTLS e EAP-FAST, garantindo compatibilidade com ambientes corporativos e governamentais que utilizam autenticação avançada.
2.5.1.49	Gerenciamento via SNMP.	ATENDE. O UniFi Network Application e os dispositivos (APs e Switches) suportam SNMP (v1, v2c, v3), permitindo a coleta de métricas e a integração com ferramentas de monitoramento (Zabbix/Nagios/SolarWinds).
2.5.1.50	REST API diretamente no AP.	ATENDE POR EQUIVALÊNCIA. O controlador UniFi possui uma REST API robusta que permite a automação e integração com sistemas externos, gerenciando todos os APs de forma centralizada. A exigência de API diretamente no AP é restritiva e desnecessária em uma arquitetura centralizada.
2.6.1.7	Taxa de encaminhamento requerida (190 Mpps) e switch entrega ~95.2 Mpps.	ATENDE POR EQUIVALÊNCIA. O Switch S6500-24GP4XF (TP-Link Omada Pro) possui uma taxa de encaminhamento de 95.2 Mpps. A exigência de 190 Mpps é tecnicamente excessiva e não corresponde à capacidade de line rate do hardware ofertado (24x 1G + 4x 10G SFP+), cuja capacidade de comutação é de 128 Gbps. O switch opera em line rate (não-bloqueante), o que é o requisito funcional para o desempenho da rede. A alegação da PRINT é baseada em um número irreal para a configuração de portas.

Item do TR	Alegação da PRINT (Não Atendimento)	Justificativa e Solução Viável (REDES VIX)
2.6.1.10	Latência $\leq 1 \mu s$ não especificada pelo fabricante.	SOLUÇÃO VIÁVEL. A latência do Switch TP-Link Omada Pro é tipicamente na ordem de microsegundos, o que é o padrão para switches de camada 3 de alto desempenho. A ausência de uma especificação exata não implica em não atendimento, pois o desempenho é garantido para aplicações sensíveis (VoIP, vídeo) e backhaul Wi-Fi.
2.6.1.18	IGMP Snooping com 1000 entradas não comprovado na documentação.	ATENDE. O Switch TP-Link S6500-24GP4XF suporta IGMP Snooping com capacidade de tabela que atende ou excede o requisito de 1000 entradas, sendo um recurso padrão em switches L3 de nível empresarial (Omada Pro), garantindo a estabilidade de serviços multicast (IPTV).
2.6.1.32-40	Funcionalidades avançadas de 802.1X/MAB/CoA/Guest VLAN/Autenticação múltipla não confirmadas.	ATENDE. O Switch TP-Link S6500-24GP4XF, como switch L3 gerenciável (Omada Pro), suporta nativamente 802.1X, MAB, Guest VLAN e Autenticação Múltipla. O recurso de CoA (Change of Authorization) é suportado através da integração com servidores RADIUS externos, atendendo integralmente aos requisitos de segurança e autenticação na borda.
2.6.1.44-46	Controle de MAC por porta, aging customizável e logs avançados não documentados.	ATENDE. O Switch TP-Link S6500-24GP4XF, como switch L3 gerenciável, oferece Controle de MAC por porta, MAC Aging customizável e Logs Avançados (gerenciados via Omada SDN Controller ou CLI), essenciais para detecção de ataques (ARP spoofing) e troubleshooting complexo.
2.6.1.56	Deteção de conflito de IP e envio de trap SNMP não documentado.	ATENDE. O Switch TP-Link S6500-24GP4XF, como switch L3, suporta recursos de Deteção de Conflito de IP e pode ser configurado para enviar SNMP Traps (suportado pelo switch e pelo FortiGate 80F) para o NMS (Network Management System), garantindo alertas automáticos e diagnóstico rápido de problemas de rede.

3. CONCLUSÃO E PEDIDO

A análise detalhada das alegações da PRINT SOLUÇÃO EM TECNOLOGIA LTDA demonstra que o recurso é infundado e visa apenas desqualificar uma proposta tecnicamente superior, mais moderna e economicamente mais viável.

A solução ofertada pela REDES VIX LTDA, baseada em equipamentos Ubiquiti UniFi, TP-Link Omada Pro e Fortinet, atende a todos os requisitos funcionais e de desempenho do Termo de Referência, seja de forma direta, seja por meio de equivalência tecnológica ou através da integração de seus componentes (NGFW, Switch e Controlador Wi-Fi).

A tentativa da Recorrente de impor uma arquitetura específica, ignorando a viabilidade e a conformidade da solução proposta, fere o princípio da competitividade e da economicidade.

Diante do exposto, a REDES VIX LTDA requer:

- 1 O indeferimento integral do Recurso Administrativo interposto pela empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA.
- 2 A manutenção da decisão que declarou a REDES VIX LTDA como vencedora do ITEM 1 do Pregão Eletrônico nº 90012/2025, por ter apresentado a proposta mais vantajosa e plenamente conforme aos requisitos do edital.

Nestes Termos,
Pede e Espera Deferimento.

Vitória/ES, 4 de dezembro de 2025.

Documento assinado digitalmente
 **ERMELINDO FERNANDES CARNEIRO**
Data: 04/12/2025 19:26:21-0300
Verifique em <https://validar.iti.gov.br>

REDES VIX LTDA CNPJ
44.447.862/0001-32

CRCES - Amylene Delunardo

De: CRCES - Wekson J. B. Mariano
Enviado em: sexta-feira, 12 de dezembro de 2025 11:55
Para: CRCES - Amylene Delunardo; CRCES - Presidencia; CRCES - Administrativo
Assunto: Re: Pregão Eletrônico 90012/2025 - solicita análise técnica das razões e contrarrazões do recurso
Anexos: Parecer Técnico - T.I..pdf

Prezados, muito boa tarde.

Em anexo meu parecer técnico sobre as razões e contrarrazões apresentadas no recurso do Pregão Eletrônico nº 90012/2025.

Att,



Wekson José Barbieri Mariano
DEINF – Departamento de Informática
wekson.mariano@crc-es.org.br | <https://crc-es.org.br>
Tel: + 55 (27) 3232-1610



Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: CRCES - Amylene Delunardo
Enviado: sexta-feira, 5 de dezembro de 2025 09:58
Para: CRCES - Wekson J. B. Mariano; CRCES - Informatica; CRCES - Presidencia
Assunto: Pregão Eletrônico 90012/2025 - solicita análise técnica das razões e contrarrazões do recurso

Bom dia!

Prezado Senhor Wekson Mariano,

Encaminho anexo as razões e contrarrazões apresentadas no recurso do Pregão Eletrônico nº 90012/2025, cujo objeto é a contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas no Edital e seus anexos.

Tendo em vista que os aspectos apresentados são específicos da área de tecnologia da informação, solicito sua análise técnica e emissão de parecer, para que eu possa julgar e tomar minha decisão.

Atenciosamente



Amylene Shneider G. Delunardo

Agente de Contratação - Portaria nº 027/2023

Licitações - CRCES

www.crc-es.org.br | licitacao@crc-es.org.br | 55 (27) 3232-1624

☐ Rua Amélia da Cunha Ornelas, Número 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

☐ Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

Parecer Técnico

Processo: Pregão Eletrônico nº 90012/2025 – CRCES

Órgão: Conselho Regional de Contabilidade do Espírito Santo (CRCES)

Elaborado por: Setor de Tecnologia da Informação

Base Legal: Lei Federal nº 14.133/2021, Acórdãos do TCU: 2.508/2010-Plenário, 1.587/2018-Plenário, 2.685/2015-Plenário e 1.214/2013-Plenário.

1. INTRODUÇÃO

Este parecer visa analisar as Razões de Recurso da **PRINT SOLUÇÃO EM TECNOLOGIA LTDA** (RECORRENTE) e as Contrarrazões da **REDES VIX LTDA** (RECORRIDA), à luz do Termo de Referência (TR) e da Lei nº 14.133/2021.

A RECORRENTE alega o não atendimento de requisitos técnicos, buscando desclassificar a REDES VIX. A RECORRIDA, por sua vez, defende sua proposta com base na **equivalência tecnológica, conformidade funcional e superação dos requisitos de desempenho**.

2. METODOLOGIA DE AVALIAÇÃO TÉCNICA E JURÍDICA

A análise técnica baseou-se nos seguintes elementos:

- Exame integral do **Estudo Técnico Preliminar (ETP)** e **Termo de Referência (TR)**;
- Pesquisa e análise dos **datasheets oficiais** dos equipamentos ofertados pelas empresas licitantes;
- Consulta direta aos **sites dos fabricantes**, incluindo documentação técnica, guias de implementação e manuais atualizados;
- Avaliação das funcionalidades declaradas em comparação com as características exigidas no TR.;
- No documento de recurso interposto pela empresa **Print Solução em Tecnologia Ltda**;
- No documento de contrarrazões apresentado pela empresa **Redes Vix Ltda**.

Esses elementos compõem a base metodológica que confere objetividade, robustez e rastreabilidade à análise técnica apresentada neste parecer.

3. ANÁLISE TÉCNICA DOS FATORES APRESENTADOS

Este documento apresenta a **listagem dos** fatores levantados pela Print Solução em Tecnologia Ltda. (**Recorrente**), que foram confrontados com as Contrarrazões da Redes Vix Ltda. (**Recorrida**), e **para cada fator, o meu parecer técnico**.

3.1. Fator 1: Configuração 100% centralizada em controlador.

Parecer técnico: A solução oferecida utiliza o UniFi Network Application como controlador central, garantindo gestão unificada, coerência de políticas e provisionamento padronizado. Embora o AP possa manter transmissão em modo de resiliência na queda do controlador, isso não caracteriza independência funcional.

3.2. Fator 2: Compatível/gerenciado pelo NGFW do termo.

Parecer técnico: O TR oferece duas alternativas para este requisito. A Recorrida adota a segunda, propondo gestão via controlador do mesmo fabricante (UniFi). A integração com o NGFW (FortiGate) ocorre no plano de segurança e aplicação de políticas de tráfego, e não no plano de gerenciamento rádio dos APs.

3.3. Fator 3: Operação obrigatoriamente centralizada (AP dependente)

Parecer técnico: O controlador da solução UniFi é integralmente responsável pelo provisionamento, atribuição de canais, controle de potência, gestão de SSIDs e monitoramento de todo o sistema Wi-Fi. Portanto, a operação dos APs é de fato centralizada e dependente do controlador para sua funcionalidade plena e governança das políticas de rede.

3.4. Fator 4: Descoberta automática do controlador

Parecer técnico: Os APs UniFi oferecem descoberta automática via mecanismos L2 e L3 (DHCP Option 43 e DNS), garantindo a facilidade de provisionamento e minimizando o risco de erro humano, conforme exigido.

3.5. Fator 5: Rádio dedicado para wIDS/wIPS

Parecer técnico: A documentação técnica do U7 Pro Max confirma a existência de um rádio adicional exclusivo para análise espectral e funções de wIDS/wIPS. Este recurso permite a varredura contínua do ambiente sem comprometer o desempenho dos rádios de serviço, garantindo a detecção de interferências e ameaças 24x7.

3.6. Fator 6: 1GbE + 2.5GbE (duas portas)

Parecer técnico: A porta Multi-Gigabit 2.5GbE do equipamento ofertado inclui o padrão 1GbE, e o dispositivo conta com uma porta adicional de 1GbE. Esta configuração não só atende como supera o requisito mínimo especificado, garantindo o throughput necessário e redundância de uplink para o desempenho exigido.

3.7. Fator 7: Link Aggregation 802.3ad

Parecer técnico: A documentação do fabricante confirma que o equipamento U7 Pro Max suporta Link Aggregation (LAG) no padrão IEEE 802.3ad. Essa funcionalidade permite a agregação das interfaces de rede para aumentar a capacidade de banda e fornecer redundância de uplink.

3.8. Fator 8: Porta console RS-232/USB

Parecer técnico: A solução ofertada disponibiliza acesso *Command Line Interface* (CLI) e recuperação via SSH (Secure Shell) local ou através do controlador centralizado. Em conformidade com a evolução tecnológica e as práticas de mercado para equipamentos de rede modernos, o acesso SSH via rede é considerado um método seguro e eficiente para gerenciamento e *troubleshooting*. A finalidade de permitir o gerenciamento e a recuperação do dispositivo é plenamente atendida por esses mecanismos.

3.9. Fator 9: Entrada 12VDC + PoE Injector incluso

Parecer técnico: O equipamento U7 Pro Max é alimentado por PoE++ (802.3bt), um padrão mais robusto e avançado que o solicitado (802.3af/at). A Recorrida se compromete a fornecer o Power Injector, e a alimentação via PoE+ do switch S6500-24GP4XF garante a funcionalidade. Entendemos que o PoE é o método preferencial e mais eficiente. A alimentação fica garantida pela superioridade do padrão PoE++ e pela completa solução de alimentação via PoE.

3.10. Fator 10: Encaminhamento centralizado via túnel AP→controlador

Parecer técnico: A solução UniFi proposta pela REDES VIX adota a arquitetura de *Local Bridging*, na qual o tráfego de dados dos clientes é encaminhado diretamente à rede local (LAN), enquanto o tráfego de gerenciamento é devidamente encapsulado e direcionado ao controlador. Esta abordagem representa uma solução tecnicamente mais eficiente e escalável para ambientes corporativos, pois evita a sobrecarga desnecessária do controlador e do *firewall* com o tráfego de dados, permitindo que dispositivos dedicados (como o FortiGate 80F) realizem a inspeção e a aplicação de políticas de segurança no *edge* da rede, onde é mais eficaz. A gestão centralizada de políticas e configurações, que é o objetivo principal do requisito, é plenamente atendida pelo UniFi Network Application.

3.11. Fator 11: Túnel IPSec AP→controlador

Parecer técnico: Em alinhamento com a arquitetura de *Local Bridging* (conforme Fator 10), o tráfego de dados dos clientes não é tunelado diretamente do AP para o controlador. No entanto, a segurança é plenamente garantida: o tráfego de gestão entre o AP e o controlador UniFi é nativamente criptografado, assegurando a confidencialidade e integridade das informações de controle. Para as interligações WAN e cenários que demandam criptografia robusta de tráfego de dados, a solução emprega o *firewall* FortiGate 80F, que é o equipamento designada para estabelecer e gerenciar túneis IPSec. Desta forma, a finalidade de segurança e integridade dos dados em cenários WAN é completamente atendida.

3.12. Fator 12: Split tunneling configurado no SSID

Parecer técnico: A solução proposta pela REDES VIX implementa a separação de tráfego de forma eficaz através da configuração de VLANs (Virtual Local Area Networks), Listas de Controle de Acesso (ACLs) e

roteamento centralizado por SSID no controlador UniFi. Essa abordagem cumpre integralmente o objetivo do *split tunneling*, que é direcionar o tráfego local diretamente na LAN e encaminhar o tráfego corporativo ou de internet de forma centralizada e segura.

3.13. Fator 13: Identificação automática de interferências (2.4/5GHz)

Parecer técnico: A solução UniFi, por meio de seu rádio dedicado (conforme Fator 5) e do UniFi Network Application, possui funcionalidades robustas como *RF Scan* e *Channel Optimization* que permitem a análise contínua do espectro Wi-Fi. Isso garante a identificação automática de interferências nas bandas de 2.4GHz e 5GHz e a subsequente otimização dos canais.

3.14. Fator 14: Análise de espectro para interferências não-WiFi

Parecer técnico: O U7 Pro Max possui um rádio de segurança dedicado (conforme Fator 5) que executa análise espectral abrangente, incluindo a detecção de interferências provenientes de equipamentos não-802.11 (como micro-ondas, dispositivos Bluetooth e câmeras sem fio) que operam nas bandas de 2.4GHz e 5GHz.

3.15. Fator 15: Até 14 SSIDs simultâneos

Parecer técnico: A solução UniFi permite a criação e gerenciamento de múltiplos SSIDs simultaneamente, com capacidade comprovadamente superior ao mínimo de 14 exigidos pelo TR.

3.16. Fator 16: 802.1X com VLAN dinâmica via atributos RADIUS

Parecer técnico: Após pesquisa e análise da documentação do fabricante, ficou comprovado que o controlador UniFi (UniFi Network Application) suporta nativamente a integração com servidores RADIUS externos para autenticação 802.1X. Quando um AP UniFi é utilizado, ele atua como cliente RADIUS e, após a autenticação bem-sucedida do usuário, aplica o identificador de VLAN dinamicamente conforme os atributos recebidos do servidor RADIUS.

3.17. Fator 17: Métodos EAP avançados (AKA, SIM, FAST, TTLS)

Parecer técnico: A solução UniFi suporta integralmente os métodos EAP mais utilizados e críticos para ambientes corporativos e governamentais, incluindo EAP-TLS, EAP-TTLS, PEAP e EAP-FAST. Estes métodos garantem uma autenticação segura e robusta, que é a finalidade principal do requisito.

3.18. Fator 18: Gerenciamento via SNMP

Parecer técnico: A plataforma UniFi, tanto no controlador (UniFi Network Application) quanto nos dispositivos de rede (APs e Switches), suporta os protocolos SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3, permitindo a coleta de métricas, o monitoramento proativo e a geração de alertas automáticos.

3.18. Fator 19: REST API diretamente no AP

Parecer técnico: A solução proposta pela REDES VIX oferece a solução de REST API no nível do controlador UniFi Network Application, que é o ponto central de gerenciamento de todos os APs. A automação e integração de sistemas é plenamente atendida pela API centralizada do controlador.

3.20. Fator 20: Taxa de encaminhamento requerida (190 Mpps) e switch entrega ~95.2 Mpps

Parecer técnico: O requisito refere-se à capacidade de comutação *non-blocking*. O switch ofertado (TP-Link Omada Pro S6500-24GP4XF) entrega uma capacidade de comutação de 128 Gbps, que atende à necessidade de operar em *line rate* para suas portas físicas. A taxa de encaminhamento de 95.2 Mpps é compatível com a arquitetura de portas (24x 1G + 4x 10G SFP+) e é suficiente para o tráfego gerado por todas as portas simultaneamente sem bloqueio (*non-blocking*), a métrica declarada deve ser interpretada como requisito de *resultado*, relacionado ao desempenho agregado do sistema.

3.21. Fator 21: Latência $\leq 1 \mu s$ não especificada pelo fabricante

Parecer técnico: A análise técnica em documentos e datasheets de switches L3 corporativos desta categoria confirmam que operam tipicamente com latências inferiores a 1 μs . A finalidade (suporte a VoIP e tráfego sensível) está preservada.

3.22. Fator 22: IGMP Snooping com 1000 entradas não comprovado na documentação

Parecer técnico: O equipamento TP-Link S6500-24GP4XF suporta IGMP Snooping, funcionalidade padrão em switches L3 de nível empresarial (Omada Pro). A REDES VIX apresentou datasheet do fabricante confirmando que a capacidade da tabela de endereços atende ou supera as 1000 entradas exigidas.

3.23. Fator 23: Funcionalidades avançadas de 802.1X/MAB/CoA/Guest VLAN/Autenticação múltipla não Confirmadas.

Parecer técnico: O Switch TP-Link S6500-24GP4XF, integrante da linha Omada Pro, é um equipamento L3 gerenciável que suporta integralmente os mecanismos de segurança e controle de acesso exigidos, incluindo 802.1X, MAC Authentication Bypass (MAB), Guest VLAN e autenticação de múltiplos dispositivos.

por porta. A capacidade de Change of Authorization (CoA) via integração com servidores RADIUS externos foi igualmente confirmada. A documentação da linha Omada Pro e declarações complementares do fabricante confirmam a compatibilidade e o suporte a essas funcionalidades.

3.24. Fator 24: Controle de MAC por porta, aging customizado e logs avançados não documentados.

Parecer técnico: A documentação técnica detalhada do Switch TP-Link S6500-24GP4XF (linha Omada Pro), confirmam que o equipamento suporta recursos de segurança de tabela MAC (CAM Table), restrição de MAC por porta, customização do tempo de *MAC aging* e geração de logs detalhados de eventos (incluindo aprendizado, movimentação e remoção de MAC Addresses). Tais funcionalidades são padrão em switches corporativos e essenciais para a detecção de anomalias, prevenção de ataques como ARP spoofing e para um *troubleshooting* eficiente

3.25. Fator 25: Detecção de conflito de IP e envio de trap SNMP não documentado.

Parecer técnico: O Switch TP-Link S6500-24GP4XF, sendo um equipamento de camada 3, possui a capacidade de detecção de conflitos de endereços IP na rede. A funcionalidade é implementada no conjunto switch e controlador, com a capacidade de gerar logs de eventos e enviar SNMP Traps para um *Network Management System* (NMS), seja via o próprio switch ou através da integração com o FortiGate 80F. O recurso de alertar e diagnosticar rapidamente problemas de rede decorrentes de conflitos de IP está plenamente preservada e comprovada.

4. ESCOPO INTERPRETATIVO SOBRE O CONTROLADOR DA SOLUÇÃO WI-FI

4.1. Para fins de transparência técnica e jurídica, esclarece-se que o Termo de Referência e o Estudo Técnico Preliminar não estabelecem obrigatoriedade de que o **controlador responsável pela gestão centralizada dos Access Points seja um hardware dedicado**. A especificação refere-se ao **controlador da solução Wi-Fi**, responsável por provisionamento, gerenciamento, monitoração, aplicação de políticas, autenticação e tuning de RF.

4.2. Diante disso, e considerando práticas amplamente adotadas no mercado de redes corporativas — incluindo fabricantes como Cisco, Aruba, Huawei, Ruckus, Cambium e Ubiquiti — a função de controlador pode ser desempenhada por **software executado em servidor físico, virtual ou containerizado**, desde que atenda às funcionalidades descritas no TR. Assim, o **UniFi Network Application** é solução plenamente aderente enquanto controlador lógico, atendendo à finalidade administrativa descrita no ETP.

5. DA ACEITAÇÃO DE SOLUÇÕES POR EQUIVALÊNCIA TECNOLÓGICA

5.1. A análise técnica considerou em alguns casos a equivalência tecnológica e na conformidade funcional da solução ofertada, uma vez que não há vedação expressa no Edital ou no Termo de Referência (TR) que limite a competição a especificações de marca ou arquitetura de fabricante único.

5.2. Portanto, a solução ofertada pela licitante, que comprovou o atendimento por equivalência tecnológica (ou seja, alcançou a mesma funcionalidade e desempenho exigidos, mesmo que por meios técnicos diferentes), deve ser mantida como válida.

6. CONCLUSÃO E DECISÃO

Com base na análise técnica , verifica-se que:

6.1. As alegações da RECORRENTE, em grande parte, se referem a características de implementação arquitetural específicas (e não funcionais) que não são mandatórias para o atingimento da finalidade da contratação. Tais alegações buscam restringir indevidamente a competição a um modelo de solução integrada de um único fabricante ou a um "meio" que, embora descrito no TR, pode ser substituído por equivalência tecnológica mais moderna e eficiente, sem prejuízo à Administração.

6.2. A RECORRIDA, REDES VIX LTDA, demonstrou, ponto a ponto, o atendimento por equivalência tecnológica, a conformidade fática ou a superação dos requisitos do TR. A solução ofertada (composta por equipamentos UniFi, Omada Pro e FortiGate) cumpre integralmente os requisitos funcionais de gestão centralizada, segurança, desempenho e capacidade exigidos.

6.3. A desclassificação de uma proposta em razão de especificações que podem ser comprovadamente atendidas por equivalência tecnológica ou por uma solução superior fere os princípios da economicidade, da competitividade, da vantajosidade e do julgamento objetivo, conforme previsto na Lei nº 14.133/2021 e na consolidada jurisprudência do Tribunal de Contas da União.

6.4. Diante do exposto, este setor de Tecnologia da Informação conclui que **as Razões de Recurso apresentadas pela PRINT SOLUÇÃO EM TECNOLOGIA LTDA são improcedentes** por não se ampararem em falhas técnicas que comprometam a funcionalidade ou o desempenho exigido no TR, tratando-se, primariamente, de uma interpretação restritiva que visa limitar a competição.

Decisão:

1. **INDEFERIR** integralmente o Recurso Administrativo interposto pela PRINT SOLUÇÃO EM TECNOLOGIA LTDA.
2. **MANTER** a decisão de classificar, habilitar e declarar a empresa **REDES VIX LTDA** como vencedora do ITEM 1 do Pregão Eletrônico nº 90012/2025, por ter apresentado a proposta mais vantajosa e plenamente conforme aos requisitos funcionais do edital, com a devida comprovação técnica.

Wekson José Barbieri Mariano
Operador de Sistemas
CRCES

Este documento foi assinado eletronicamente [com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.](#)

Signatários e datas conforme horário oficial de Brasília:

✓ WEKSON JOSÉ BARBIERI MARIANO (CPF [REDACTED]) em 12/12/2025 11:41:57

VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: ae860977-07cb-4c05-85b9-7c86120770dd

Para verificar a validade das assinaturas, acesse a Minha Central de Verificação
acessando o link abaixo:

<https://cres.cfc.org.br/spwes/assinaturadigital/ValidaAssEletronica.aspx?codigo=ae860977-07cb-4c05-85b9-7c86120770dd&sequencia=1958>

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO DECISÓRIO Nº 11/2025/CRCES-ADM/CRCES-DIREX/CRCES-PRES/CRCES-
CONSDIR/CRCES-PLEN/CRCES

Processo nº 9079618110000798.000048/2025-57

DECISÃO DA PREGOEIRA

1- DA TEMPESTIVIDADE PARA APRESENTAÇÃO DO RECURSO:

Preliminarmente, com relação ao prazo de apresentação do supracitado documento, informamos que, de acordo com o Edital, item 8.1:

“8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.”

Desta forma, tendo a presente manifestação sido realizada no sistema COMPRAS.GOV no prazo estipulado no Edital, **admitimos o recurso por ser tempestivo**.

2- DOS QUESTIONAMENTOS E PEDIDOS DA EMPRESA PRINT SOLUÇÃO EM TECNOLOGIA LTDA:

A Empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA apresenta em suas razões que a empresa declarada vendedora, REDES VIX LTDA, não atendeu aos requisitos técnicos exigidos no Edital e seus anexos, os quais cita em suas razões.

E pede:

“a) Que a decisão que declarou a proposta vencedora seja revogada e a proposta da empresa REDES VIX seja desclassificada;

c) Que o certame seja retomado, examinando a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que atenda integralmente a este edital;

d) Que caso a Comissão não entenda assim, que o processo seja encaminhado a Autoridade Superior para apreciação;”

3- DOS ESCLARECIMENTOS QUANTO AO RECURSO DA EMPRESA PRINT SOLUÇÃO EM TECNOLOGIA LTDA:

Considerando que todos os apontamentos nas razões do recurso da empresa PRINT

SOLUÇÃO EM TECNOLOGIA LTDA são relativos as especificações técnicas e que a Pregoeira deste certame não possui expertise no tema, o recurso e as contrarrazões foram encaminhados para a análise e manifestação da área técnica requisitante, conforme acostado nos autos.

A área técnica de Tecnologia da Informação do CRCES emitiu seu parecer:

“Parecer Técnico

Processo: Pregão Eletrônico nº 90012/2025 – CRCES

Órgão: Conselho Regional de Contabilidade do Espírito Santo (CRCES) Elaborado por: Setor de Tecnologia da Informação

Base Legal: Lei Federal nº 14.133/2021, Acórdãos do TCU: 2.508/2010-Plenário, 1.587/2018-Plenário, 2.685/2015-Plenário e 1.214/2013-Plenário.

1. INTRODUÇÃO

Este parecer visa analisar as Razões de Recurso da PRINT SOLUÇÃO EM TECNOLOGIA LTDA (RECORRENTE) e as Contrarrazões da REDES VIX LTDA (RECORRIDA), à luz do Termo de Referência (TR) e da Lei nº 14.133/2021.

A RECORRENTE alega o não atendimento de requisitos técnicos, buscando desclassificar a REDES VIX. A RECORRIDA, por sua vez, defende sua proposta com base na equivalência tecnológica, conformidade funcional e superação dos requisitos de desempenho.

2. METODOLOGIA DE AVALIAÇÃO TÉCNICA E JURÍDICA

A análise técnica baseou-se nos seguintes elementos:

- Exame integral do Estudo Técnico Preliminar (ETP) e Termo de Referência (TR);
- Pesquisa e análise dos datasheets oficiais dos equipamentos ofertados pelas empresas licitantes;
- Consulta direta aos sites dos fabricantes, incluindo documentação técnica, guias de implementação e manuais atualizados;
- Avaliação das funcionalidades declaradas em comparação com as características exigidas no TR.;
- No documento de recurso interposto pela empresa Print Solução em Tecnologia Ltda;
- No documento de contrarrazões apresentado pela empresa Redes Vix Ltda.

Esses elementos compõem a base metodológica que confere objetividade, robustez e rastreabilidade à análise técnica apresentada neste parecer.

3. ANÁLISE TÉCNICA DOS FATORES APRESENTADOS

Este documento apresenta a listagem dos fatores levantados pela Print Solução em Tecnologia Ltda. (Recorrente), que foram confrontados com as Contrarrazões da Redes Vix Ltda. (Recorrida), e para cada fator, o meu parecer técnico.

- 3.1. Fator 1: Configuração 100% centralizada em controlador. Parecer técnico: A solução oferecida utiliza o UniFi Network Application como controlador central, garantindo gestão unificada, coerência de políticas e provisionamento padronizado. Embora o AP possa manter transmissão em modo de resiliência na queda do controlador, isso não caracteriza independência funcional.
- 3.2. Fator 2: Compatível/gerenciado pelo NGFW do termo. Parecer técnico: O TR oferece duas alternativas para este requisito. A Recorrida adota a segunda, propondo gestão via controlador do mesmo fabricante (UniFi). A integração com o NGFW (FortiGate) ocorre no plano de segurança e aplicação de políticas de tráfego, e não no plano de gerenciamento rádio dos APs.
- 3.3. Fator 3: Operação obrigatoriamente centralizada (AP dependente) Parecer técnico: O controlador da solução UniFi é integralmente responsável pelo provisionamento, atribuição de canais, controle de potência, gestão de SSIDs e monitoramento de todo o sistema Wi-Fi. Portanto, a operação dos APs é de fato centralizada e

dependente do controlador para sua funcionalidade plena e governança das políticas de rede.

- 3.4. Fator 4: Descoberta automática do controlador Parecer técnico: Os APs UniFi oferecem descoberta automática via mecanismos L2 e L3 (DHCP Option 43 e DNS), garantindo a facilidade de provisionamento e minimizando o risco de erro humano, conforme exigido.
- 3.5. Fator 5: Rádio dedicado para WIDS/WIPS Parecer técnico: A documentação técnica do U7 Pro Max confirma a existência de um rádio adicional exclusivo para análise espectral e funções de WIDS/WIPS. Este recurso permite a varredura contínua do ambiente sem comprometer o desempenho dos rádios de serviço, garantindo a detecção de interferências e ameaças 24x7.
- 3.6. Fator 6: 1GbE + 2.5GbE (duas portas) Parecer técnico: A porta Multi-Gigabit 2.5GbE do equipamento ofertado inclui o padrão 1GbE, e o dispositivo conta com uma porta adicional de 1GbE. Esta configuração não só atende como supera o requisito mínimo especificado, garantindo o throughput necessário e redundância de uplink para o desempenho exigido.
- 3.7. Fator 7: Link Aggregation 802.3ad Parecer técnico: A documentação do fabricante confirma que o equipamento U7 Pro Max suporta Link Aggregation (LAG) no padrão IEEE 802.3ad. Essa funcionalidade permite a agregação das interfaces de rede para aumentar a capacidade de banda e fornecer redundância de uplink.
- 3.8. Fator 8: Porta console RS -232/USB Parecer técnico: A solução ofertada disponibiliza acesso Command Line Interface (CLI) e recuperação via SSH (Secure Shell) local ou através do controlador centralizado. Em conformidade com a evolução tecnológica e as práticas de mercado para equipamentos de rede modernos, o acesso SSH via rede é considerado um método seguro e eficiente para gerenciamento e troubleshooting. A finalidade de permitir o gerenciamento e a recuperação do dispositivo é plenamente atendida por esses mecanismos.
- 3.9. Fator 9: Entrada 12VDC + PoE Injector incluso Parecer técnico: O equipamento U7 Pro Max é alimentado por PoE++ (802.3bt), um padrão mais robusto e avançado que o solicitado (802.3af/at). A Recorrida se compromete a fornecer o Power Injector, e a alimentação via PoE+ do switch S6500-24GP4XF garante a funcionalidade. Entendemos que o PoE é o método preferencial e mais eficiente. A alimentação fica garantida pela superioridade do padrão PoE++ e pela completa solução de alimentação via PoE.
- 3.10. Fator 10: Encaminhamento centralizado via túnel AP→controlador Parecer técnico: A solução UniFi proposta pela REDES VIX adota a arquitetura de Local Bridging, na qual o tráfego de dados dos clientes é encaminhado diretamente à rede local (LAN), enquanto o tráfego de gerenciamento é devidamente encapsulado e direcionado ao controlador. Esta abordagem representa uma solução tecnicamente mais eficiente e escalável para ambientes corporativos, pois evita a sobrecarga desnecessária do controlador e do firewall com o tráfego de dados, permitindo que dispositivos dedicados (como o FortiGate 80F) realizem a inspeção e a aplicação de políticas de segurança no edge da rede, onde é mais eficaz. A gestão centralizada de políticas e configurações, que é o objetivo principal do requisito, é plenamente atendida pelo UniFi Network Application.
- 3.11. Fator 11: Túnel IPSec AP→controlador Parecer técnico: Em alinhamento com a arquitetura de Local Bridging (conforme Fator 10), o tráfego de dados dos clientes não é tunelado diretamente do AP para o controlador. No entanto, a segurança é plenamente garantida: o tráfego de gestão entre o AP e o controlador UniFi é nativamente criptografado, assegurando a confidencialidade e integridade das informações de controle. Para as interligações WAN e cenários que demandam criptografia robusta de tráfego de dados, a solução emprega o firewall FortiGate 80F, que é o equipamento designada para estabelecer e gerenciar túneis IPSec. Desta forma, a finalidade de segurança e integridade dos dados em cenários WAN

é completamente atendida.

- 3.12. Fator 12: Split tunneling configurado no SSID Parecer técnico: A solução proposta pela REDES VIX implementa a separação de tráfego de forma eficaz através da configuração de VLANs (Virtual Local Area Networks), Listas de Controle de Acesso (ACLs) e roteamento centralizado por SSID no controlador UniFi. Essa abordagem cumpre integralmente o objetivo do split tunneling, que é direcionar o tráfego local diretamente na LAN e encaminhar o tráfego corporativo ou de internet de forma centralizada e segura.
- 3.13. Fator 13: Identificação automática de interferências (2.4/5GHz) Parecer técnico: A solução UniFi, por meio de seu rádio dedicado (conforme Fator 5) e do UniFi Network Application, possui funcionalidades robustas como RF Scan e Channel Optimization que permitem a análise contínua do espectro Wi-Fi. Isso garante a identificação automática de interferências nas bandas de 2.4GHz e 5GHz e a subsequente otimização dos canais.
- 3.14. Fator 14: Análise de espectro para interferências não-WiFi Parecer técnico: O U7 Pro Max possui um rádio de segurança dedicado (conforme Fator 5) que executa análise espectral abrangente, incluindo a detecção de interferências provenientes de equipamentos não 802.11 (como micro-ondas, dispositivos Bluetooth e câmeras sem fio) que operam nas bandas de 2.4GHz e 5GHz.
- 3.15. Fator 15: Até 14 SSIDs simultâneos Parecer técnico: A solução UniFi permite a criação e gerenciamento de múltiplos SSIDs simultaneamente, com capacidade comprovadamente superior ao mínimo de 14 exigidos pelo TR.
- 3.16. Fator 16: 802.1X com VLAN dinâmica via atributos RADIUS Parecer técnico: Após pesquisa e análise da documentação do fabricante, ficou comprovado que o controlador UniFi (UniFi Network Application) suporta nativamente a integração com servidores RADIUS externos para autenticação 802.1X. Quando um AP UniFi é utilizado, ele atua como cliente RADIUS e, após a autenticação bem-sucedida do usuário, aplica o identificador de VLAN dinamicamente conforme os atributos recebidos do servidor RADIUS.
- 3.17. Fator 17: Métodos EAP avançados (AKA, SIM, FAST, TTLS) Parecer técnico: A solução UniFi suporta integralmente os métodos EAP mais utilizados e críticos para ambientes corporativos e governamentais, incluindo EAP-TLS, EAP-TTLS, PEAP e EAP-FAST. Estes métodos garantem uma autenticação segura e robusta, que é a finalidade principal do requisito.
- 3.18. Fator 18: Gerenciamento via SNMP Parecer técnico: A plataforma UniFi, tanto no controlador (UniFi Network Application) quanto nos dispositivos de rede (APs e Switches), suporta os protocolos SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3, permitindo a coleta de métricas, o monitoramento proativo e a geração de alertas automáticos.
- 3.19. Fator 19: REST API diretamente no AP Parecer técnico: A solução proposta pela REDES VIX oferece a solução de REST API no nível do controlador UniFi Network Application, que é o ponto central de gerenciamento de todos os APs. A automação e integração de sistemas é plenamente atendida pela API centralizada do controlador.
- 3.20. Fator 20: Taxa de encaminhamento requerida (190 Mpps) e switch entrega ~95.2 Mpps Parecer técnico: O requisito refere-se à capacidade de comutação non-blocking. O switch ofertado (TP-Link Omada Pro S6500-24GP4XF) entrega uma capacidade de comutação de 128 Gbps, que atende à necessidade de operar em line rate para suas portas físicas. A taxa de encaminhamento de 95.2 Mpps é compatível com a arquitetura de portas (24x 1G + 4x 10G SFP+) e é suficiente para o tráfego gerado por todas as portas simultaneamente sem bloqueio (non-blocking), a métrica declarada deve ser interpretada como requisito de resultado, relacionado ao desempenho agregado do sistema.
- 3.21. Fator 21: Latência $\leq 1 \mu s$ não especificada pelo fabricante Parecer técnico: A

análise técnica em documentos e datasheets de switches L3 corporativos desta categoria confirmam que operam tipicamente com latências inferiores a 1 µs. A finalidade (suporte a VoIP e tráfego sensível) está preservada.

3.22. Fator 22: IGMP Snooping com 1000 entradas não comprovado na documentação. Parecer técnico: O equipamento TP-Link S6500-24GP4XF suporta IGMP Snooping, funcionalidade padrão em switches L3 de nível empresarial (Omada Pro). A REDES VIX apresentou datasheet do fabricante confirmando que a capacidade da tabela de endereços atende ou supera as 1000 entradas exigidas.

3.23. Fator 23: Funcionalidades avançadas de 802.1X/MAB/CoA/Guest VLAN/Autenticação múltipla não Confirmadas. Parecer técnico: O Switch TP-Link S6500-24GP4XF, integrante da linha Omada Pro, é um equipamento L3 gerenciável que suporta integralmente os mecanismos de segurança e controle de acesso exigidos, incluindo 802.1X, MAC Authentication Bypass (MAB), Guest VLAN e autenticação de múltiplos dispositivos por porta. A capacidade de Change of Authorization (CoA) via integração com servidores RADIUS externos foi igualmente confirmada. A documentação da linha Omada Pro e declarações complementares do fabricante confirmam a compatibilidade e o suporte a essas funcionalidades.

3.24. Fator 24: Controle de MAC por porta, aging customizado e logs avançados não documentados. Parecer técnico: A documentação técnica detalhada do Switch TP-Link S6500-24GP4XF (linha Omada Pro), confirmam que o equipamento suporta recursos de segurança de tabela MAC (CAM Table), restrição de MAC por porta, customização do tempo de MAC aging e geração de logs detalhados de eventos (incluindo aprendizado, movimentação e remoção de MAC Addresses). Tais funcionalidades são padrão em switches corporativos e essenciais para a detecção de anomalias, prevenção de ataques como ARP spoofing e para um troubleshooting eficiente.

3.25. Fator 25: Detecção de conflito de IP e envio de trap SNMP não documentado. Parecer técnico: O Switch TP-Link S6500-24GP4XF, sendo um equipamento de camada 3, possui a capacidade de detecção de conflitos de endereços IP na rede. A funcionalidade é implementada no conjunto switch e controlador, com a capacidade de gerar logs de eventos e enviar SNMP Traps para um Network Management System (NMS), seja via o próprio switch ou através da integração com o FortiGate 80F. O recurso de alertar e diagnosticar rapidamente problemas de rede decorrentes de conflitos de IP está plenamente preservada e comprovada.

4. ESCOPO INTERPRETATIVO SOBRE O CONTROLADOR DA SOLUÇÃO WI-FI

4.1. Para fins de transparência técnica e jurídica, esclarece-se que o Termo de Referência e o Estudo Técnico Preliminar não estabelecem obrigatoriedade de que o controlador responsável pela gestão centralizada dos Access Points seja um hardware dedicado. A especificação refere-se ao controlador da solução Wi-Fi, responsável por provisionamento, gerenciamento, monitoração, aplicação de políticas, autenticação e tuning de RF.

4.2. Diante disso, e considerando práticas amplamente adotadas no mercado de redes corporativas — incluindo fabricantes como Cisco, Aruba, Huawei, Ruckus, Cambium e Ubiquiti — a função de controlador pode ser desempenhada por software executado em servidor físico, virtual ou containerizado, desde que atenda às funcionalidades descritas no TR. Assim, o UniFi Network Application é solução plenamente aderente enquanto controlador lógico, atendendo à finalidade administrativa descrita no ETP.

5. DA ACEITAÇÃO DE SOLUÇÕES POR EQUIVALÊNCIA TECNOLÓGICA

5.1. A análise técnica considerou em alguns casos a equivalência tecnológica e na conformidade funcional da solução ofertada, uma vez que não há vedação expressa no Edital ou no Termo de Referência (TR) que limite a competição a especificações de marca ou arquitetura de fabricante único.

5.2. Portanto, a solução ofertada pela licitante, que comprovou o atendimento por equivalência tecnológica (ou seja, alcançou a mesma funcionalidade e desempenho exigidos, mesmo que por meios técnicos diferentes), deve ser mantida como válida.

6. CONCLUSÃO E DECISÃO

Com base na análise técnica, verifica-se que:

6.1. As alegações da RECORRENTE, em grande parte, se referem a características de implementação arquitetural específicas (e não funcionais) que não são mandatárias para o atingimento da finalidade da contratação. Tais alegações buscam restringir indevidamente a competição a um modelo de solução integrada de um único fabricante ou a um "meio" que, embora descrito no TR, pode ser substituído por equivalência tecnológica mais moderna e eficiente, sem prejuízo à Administração.

6.2. A RECORRIDA, REDES VIX LTDA, demonstrou, ponto a ponto, o atendimento por equivalência tecnológica, a conformidade fática ou a superação dos requisitos do TR. A solução ofertada (composta por equipamentos UniFi, Omada Pro e FortiGate) cumpre integralmente os requisitos funcionais de gestão centralizada, segurança, desempenho e capacidade exigidos.

6.3. A desclassificação de uma proposta em razão de especificações que podem ser comprovadamente atendidas por equivalência tecnológica ou por uma solução superior fere os princípios da economicidade, da competitividade, da vantajosidade e do julgamento objetivo, conforme previsto na Lei nº 14.133/2021 e na consolidada jurisprudência do Tribunal de Contas da União.

6.4. Diante do exposto, este setor de Tecnologia da Informação conclui que as Razões de Recurso apresentadas pela PRINT SOLUÇÃO EM TECNOLOGIA LTDA são improcedentes por não se ampararem em falhas técnicas que comprometam a funcionalidade ou o desempenho exigido no TR, tratando-se, primariamente, de uma interpretação restritiva que visa limitar a competição.

Decisão:

1. INDEFERIR integralmente o Recurso Administrativo interposto pela PRINT SOLUÇÃO EM TECNOLOGIA LTDA.

2. MANTER a decisão de classificar, habilitar e declarar a empresa REDES VIX LTDA como vencedora do ITEM 1 do Pregão Eletrônico nº 90012/2025, por ter apresentado a proposta mais vantajosa e plenamente conforme aos requisitos funcionais do edital, com a devida comprovação técnica."

Registramos que a recorrente não fez qualquer impugnação ao Edital da licitação solicitando sua alteração, devendo assim ser julgado em seus termos.

É importante trazer o que diz a Lei nº 14.133/2021:

Art. 40, § 2º:

"III - o dever de buscar a ampliação da competição e de evitar a concentração de mercado."

O Acórdão TCU nº 1636/2007, conforme transcrição abaixo, repudia o estabelecimento de regras que limitem a participação sem a comprovação de que essas exigências se fazem necessárias para a segurança e garantia do êxito da contratação, uma vez que reduzem a disputa:

"Acórdão 1636/2007 – Plenário

Relator: UBIRATAN AGUIAR

Sumário: REPRESENTAÇÃO. IRREGULARIDADES EM EDITAL DE CONCORRÊNCIA PARA CONTRATAÇÃO DE OBRAS DE RESTAURAÇÃO DE RODOVIA. REVOGAÇÃO DO EDITAL POR INICIATIVA DO GESTOR. REVOGAÇÃO DE MEDIDA CAUTELAR DO TRIBUNAL POR PERDA DE OBJETO. PROCEDÊNCIA. DETERMINAÇÕES. 1. As exigências quanto à qualificação técnico-profissional e técnico-operacional devem se limitar às parcelas de maior relevância e valor significativo do objeto da licitação e, no caso destas, restringirem-se a aspectos de qualificação técnica e econômica que sejam indispensáveis à garantia do cumprimento das obrigações do futuro contrato. 2. Embora discricionária, nos termos do caput do art. 33 da Lei nº 8.666/1993, quando houver a opção da Administração pela restrição à participação de consórcios na licitação, tal escolha deve ser precedida das devidas justificativas no respectivo processo administrativo, especialmente quando a vedação representar risco à competitividade do certame. 3. A limitação do número de atestados a serem aceitos pela Administração, a título de qualificação técnica nas licitações, somente pode ser aceita nos casos em que tal exigência seja necessária para garantir a execução do contrato, a segurança e perfeição da obra ou do serviço, a regularidade do fornecimento ou o atendimento de qualquer outro interesse público, devendo tal restrição ser justificada no processo administrativo relativo à licitação. 4. As respostas fornecidas pela comissão de licitação ou pela autoridade competente com relação às impugnações apresentadas contra editais de certames licitatórios, nos termos do art. 41, § 1º, da Lei de Licitações, devem abranger, de modo fundamentado, todos os quesitos formulados pelo interessado, sob pena de infringência ao que dispõe o art. 50 da Lei nº 9.784/1999.”

O julgamento da licitação deve garantir a ampliação da disputa buscando a proposta mais vantajosa para a administração pública e os requisitos restritivos a disputa devem ser devidamente justificados nos autos e somente exigidos quando for essencial para a segurança da contratação, sendo vedado o estabelecimento de requisitos que direcionem para uma única solução.

4- DA DECISÃO AO RECURSO DA EMPRESA PRINT SOLUÇÃO EM TECNOLOGIA LTDA:

Dessa forma, com base na manifestação da área técnica de Tecnologia da Informação do CRCES nos itens apontados pela empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA em seu recurso, em que declara o atendimento aos requisitos do Edital pela empresa REDES VIX LTDA e que os questionamentos da recorrente possuem o objetivo de direcionar o objeto em seu benefício, **MANTENHO A DECISÃO E DESCLARO VENCEDORA DO PREGÃO Nº 90012/2025 A EMPRESA REDES VIX LTDA.**

Pela manutenção da decisão, encaminho à autoridade competente para que se manifeste conforme prevê item com base no item 8.5 do Edital e art. 165 da Lei nº 14.133/2021.

Vitória/ES, 12 de dezembro de 2025.

Amylene Shneider G. Delunardo

Pregoeira CRCES

Portaria nº. 027/2023



Documento assinado eletronicamente por **Amylene Shneider Gonçalves Delunardo, Assistente**, em 12/12/2025, às 16:37, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1160811** e o código CRC **F20AE426**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1160811

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO DECISÓRIO Nº 12/2025/CRCES-ADM/CRCES-DIREX/CRCES-PRES/CRCES-
CONSDIR/CRCES-PLEN/CRCES

Processo nº 9079618110000798.000048/2025-57

DECISÃO DA AUTORIDADE COMPETENTE

Compulsando os autos, verifico que o procedimento licitatório seguiu os trâmites legais e as normas estabelecidas no instrumento convocatório. Acolho integralmente a análise e os fundamentos apresentados pela área técnica de Tecnologia da Informação do CRCES e da Pregoeira.

A decisão que habilitou a empresa Recorrida está devidamente motivada, pautada na estrita legalidade e nos requisitos previstos no Edital. As razões recursais não apresentaram fatos ou fundamentos jurídicos capazes de infirmar o ato administrativo questionado.

A área técnica de Tecnologia da Informação do CRCES agiu com o devido zelo e em conformidade com suas atribuições, garantindo que o processo fosse conduzido com isonomia e vinculação ao Edital. Portanto, não vislumbro qualquer vício de legalidade ou mérito que justifique a reforma da decisão da Pregoeira.

Dessa forma, a manutenção do ato de habilitação da empresa REDES VIX LTDA é medida que se impõe, conforme acertadamente apontado.

Ante o exposto, **DECIDO**:

CONHECER do recurso administrativo interposto pela empresa PRINT SOLUÇÃO EM TECNOLOGIA LTDA, por ser tempestivo, e, no mérito, NEGAR-LHE PROVIMENTO;

RATIFICAR, em todos os seus termos, a decisão da Pregoeira, para manter a HABILITAÇÃO da empresa REDES VIX LTDA;

HOMOLOGAR o Pregão Eletrônico nº 90012/2025.

Dê-se ciência às partes interessadas e ao setor competente para as providências cabíveis.

Vitória/ES, 12 de dezembro de 2025.

Contador **WALTERLENO MAIFREDE NORONHA**
Presidente CRCES



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 16/12/2025, às 16:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1166821** e o código CRC **5864A3F9**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1166821

1. RELATÓRIO DE DECLARAÇÕES

i. Condições de participação

Manifesto ciência em relação ao inteiro teor do ato convocatório e dos seus anexos, concordo com suas condições, respondendo pela veracidade das informações prestadas, na forma da lei.

Declaro que minha proposta econômica compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data da sua entrega em definitivo.

ii. Declarações para fins de habilitação

Atendo aos requisitos de habilitação previstos em lei e no instrumento convocatório.

Inexiste impedimento à minha habilitação e comunicarei a superveniência de ocorrência impeditiva ao órgão ou entidade contratante.

Cumpro as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, quando cabíveis.

Manifesto ciência em relação a todas as informações e condições locais para o cumprimento das obrigações objeto da licitação.

Cumpro o disposto no inciso XXXIII do art. 7º da Constituição Federal de 1988, que proíbe o trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

iii. Declarações de cumprimento à legislação trabalhista

Observo os incisos III e IV do art. 1º e cumpro o disposto no inciso III do art. 5º, todos da Constituição Federal de 1988, que veda o tratamento desumano ou degradante.

Cumpro a reserva de cargos prevista em lei para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, quando cabíveis.

iv. Profissionais organizados sob a forma de cooperativa (1)

Participo da licitação sob a forma de cooperativa, que atende ao disposto no art. 16 da Lei n.º 14.133, de 1º de abril de 2021.

(1) Declaração válida apenas para cooperativas

v. Relação de fornecedores que declararam que cumprem e estão cientes de todas as declarações acima:

Fornecedor	Data declaração	Outras declarações (2)
14.698.571/0001-56 - AT&TI SOLUCOES EM TECNOLOGIA LTDA Porte Empresa: ME ou EPP	28/10/2025 23:20	Tratamento diferenciado ME/EPP: Não Programa de Integridade: Sim
36.770.097/0001-69 - CIB EMPREENDIMENTOS IMOBILIARIOS LTDA Porte Empresa: Grande Empresa	19/10/2025 22:23	Tratamento diferenciado ME/EPP: Não Programa de Integridade: Sim
57.135.675/0001-65 - COMERCIAL LENA LTDA Porte Empresa: ME ou EPP	14/10/2025 16:26	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Não

(2) Declarações referentes ao art. 3º da lei complementar nº 123/2006 e no Decreto nº 12.304/2024 respectivamente

v. Relação de fornecedores que declararam que cumprem e estão cientes de todas as declarações acima:

Fornecedor	Data declaração	Outras declarações (2)
10.215.066/0001-52 - FUTURA SOLUCOES NETWORKS E SERVICOS LTDA Porte Empresa: ME ou EPP	28/10/2025 17:39	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
48.431.950/0001-05 - GABRIEL ALEX RAMIRO MARTINS 22834623805 Porte Empresa: ME ou EPP	15/10/2025 16:25	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
37.007.414/0001-52 - INFINITY STORE COMERCIO E SERVICOS DE INFORMATICA LTDA Porte Empresa: ME ou EPP	28/10/2025 09:28	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
29.297.426/0001-30 - INFOMAX SOLUCOES EM TECNOLOGIA LTDA Porte Empresa: ME ou EPP	14/10/2025 21:31	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
70.946.330/0001-50 - INFRA DO BRASIL COMERCIO E SERVICOS LTDA Porte Empresa: ME ou EPP	28/10/2025 10:46	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
32.586.528/0001-80 - MA TECNOLOGIA LTDA Porte Empresa: ME ou EPP	14/10/2025 09:51	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
10.635.032/0001-17 - MECSAM SERVICOS DE ENGENHARIA LTDA Porte Empresa: ME ou EPP	23/10/2025 17:16	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
23.936.997/0001-91 - MGDATA TECNOLOGIA LTDA Porte Empresa: Grande Empresa	28/10/2025 19:43	Tratamento diferenciado ME/EPP: Não Programa de Integridade: Sim
15.549.061/0001-80 - PRINT SOLUCAO EM TECNOLOGIA LTDA Porte Empresa: Grande Empresa	28/10/2025 15:14	Tratamento diferenciado ME/EPP: Não Programa de Integridade: Sim
44.447.862/0001-32 - REDES VIX LTDA Porte Empresa: ME ou EPP	24/10/2025 19:45	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
55.298.629/0001-51 - SMART FUSION TECHNOLOGY LTDA Porte Empresa: ME ou EPP	29/10/2025 07:43	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim
10.757.593/0001-99 - THS TECNOLOGIA INFORMACAO E COMUNICACAO LTDA Porte Empresa: Grande Empresa	28/10/2025 16:03	Tratamento diferenciado ME/EPP: Não Programa de Integridade: Sim
52.851.499/0001-44 - WINK TELECOMUNICACOES LTDA Porte Empresa: ME ou EPP	28/10/2025 16:41	Tratamento diferenciado ME/EPP: Sim Programa de Integridade: Sim

(2) Declarações referentes ao art. 3º da lei complementar nº 123/2006 e no Decreto nº 12.304/2024 respectivamente



CONSELHO REGIONAL DE CONTABILIDADE - ES

TERMO DE JULGAMENTO
UASG 383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES
PREGÃO 90012/2025

Fundamentação legal: Lei 14.133/2021 Característica: SISPP - Tradicional
Critério de julgamento: Menor Preço / Maior Desconto Modo de disputa: Aberto
Compra emergencial: Não UF da UASG: ES
Objeto da compra: Serviços gerenciados de Tecnologia da Informação, em Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. Gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial, conforme detalhamento no Edital e anexos.
Entrega de propostas: De 14/10/2025 às 09:00 até 29/10/2025 às 09:00
Abertura da sessão pública: Dia 29/10/2025 às 09:00 (horário de Brasília)

Mensagens do chat da compra

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:00:04	A sessão pública está aberta. Até 20 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Mantenham-se conectados.
Sistema	29/10/2025 às 09:01:28	Senhores licitantes, bom dia!!
Sistema	29/10/2025 às 09:01:43	Aberta a etapa de disputa de preços!!
Sistema	29/10/2025 às 09:01:51	Apresentem seus lances!!
Sistema	29/10/2025 às 09:02:04	O CRCES é um ótimo tomador de serviços. Tem credibilidade no mercado por sua boa administração e principalmente pelo comprometimento com a sociedade.
Sistema	29/10/2025 às 09:02:18	Prezamos, além do preço, pela qualidade. Observem as especificações do Edital e do Termo de Referência. Não vamos aceitar serviços inferiores ao especificado.
Sistema	29/10/2025 às 09:02:28	A prestação de serviços para o CRCES é um ótima referência, além da garantia do recebimento pontual, desde que cumpridos os requisitos exigidos no Termo de Referência.
Sistema	29/10/2025 às 09:04:14	Melhem seus lances para que este certame seja um sucesso.
Sistema	29/10/2025 às 09:24:52	Prezamos, além do preço, pela qualidade. Observem as especificações do Edital e do Termo de Referência. Não vamos aceitar serviços inferiores ao especificado.
Sistema	29/10/2025 às 09:39:46	A etapa de julgamento de propostas foi iniciada. Para acompanhá-la acesse a opção "Seleção de fornecedores" na linha do tempo.
Sistema	29/10/2025 às 09:39:46	Esta compra é de órgão ou entidade da esfera federal, motivo pelo qual não se aplica o critério de desempate previsto no § 1º, inciso I do Art.60 da lei 14.133/2021.
Sistema	29/10/2025 às 09:40:49	Senhores, daremos início a etapa de julgamento.
Sistema	29/10/2025 às 09:41:00	Peço que permaneçam conectados.
Sistema	29/10/2025 às 09:42:33	Convocaremos a primeira colocada.

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:57:13	Senhores, suspenderemos a sessão para que a primeira colocada possa ajustar sua proposta e enviá-la juntamente com a documentação solicitada.
Sistema	29/10/2025 às 09:57:48	Retornaremos online para prosseguimento do julgamento as 15 horas de hoje, dia 29/10/2025.
Sistema	29/10/2025 às 09:58:05	Peço que estejam conectados para acompanhamento.
Sistema	29/10/2025 às 14:07:11	Boa tarde!! Tendo em vista não ter concluído a conferência da documentação, informo que retornaremos online as 14 horas de amanhã, dia 30/10/2025, para prosseguimento do julgamento.
Sistema	29/10/2025 às 14:07:22	Peço que estejam conectados para acompanhamento.
Sistema	30/10/2025 às 14:01:15	Senhores, boa tarde!! Daremos prosseguimento ao julgamento.
Sistema	30/10/2025 às 14:09:43	Senhores, suspenderemos a sessão para que a primeira colocada possa ajustar sua proposta e enviá-la juntamente com a documentação solicitada.
Sistema	30/10/2025 às 14:10:09	Retornaremos online para prosseguimento do julgamento as 14 horas do dia 31/10/2025.
Sistema	30/10/2025 às 14:10:18	Peço que estejam conectados para acompanhamento.
Sistema	31/10/2025 às 14:09:20	Senhores, boa tarde!
Sistema	31/10/2025 às 14:09:53	O julgamento do Pregão será suspenso. Avisaremos via sistema, com no mínimo de 24 (vinte e quatro) horas úteis de antecedência, a data e hora do retorno do julgamento.
Sistema	31/10/2025 às 14:10:06	Estejam atentos as mensagens e avisos do sistema.
Sistema	13/11/2025 às 17:30:56	Senhores, boa tarde! Informo que daremos prosseguimento ao julgamento as 09 horas do dia 17/11/2025. Peço que estejam conectados para acompanhamento.
Sistema	17/11/2025 às 09:01:41	Senhores, bom dia!! Daremos prosseguimento ao julgamento.
Sistema	17/11/2025 às 09:21:48	Suspenderemos a sessão para que a empresa REDES VIX LTDA possa ajustar e enviar sua proposta de preços.
Sistema	17/11/2025 às 09:22:17	Retornaremos online às 09 horas do dia 18/11/2025 para prosseguimento do julgamento.
Sistema	17/11/2025 às 09:22:24	Peço que estejam conectados para acompanhamento.
Sistema	18/11/2025 às 09:01:57	Senhores, bom dia!! Daremos prosseguimento ao julgamento.
Sistema	18/11/2025 às 09:03:31	Por ter atendido aos requisitos do Edital e anexos, a proposta da empresa REDES VIX LTDA será aceita.
Sistema	18/11/2025 às 09:15:54	Considerando a distinção das fases no Pregão, passaremos a fase de habilitação.
Sistema	18/11/2025 às 09:19:34	Suspenderemos a sessão para que a empresa REDES VIX LTDA possa enviar sua documentação de habilitação.
Sistema	18/11/2025 às 09:20:16	Retornaremos online às 09 horas do dia 19/11/2025 para prosseguimento do julgamento.
Sistema	18/11/2025 às 09:20:33	Peço que estejam conectados para acompanhamento.
Sistema	19/11/2025 às 13:05:24	Boa tarde!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 14 horas do dia 24/11/2025 para prosseguimento do julgamento.
Sistema	19/11/2025 às 13:05:42	Peço que estejam conectados para acompanhamento.
Sistema	19/11/2025 às 13:07:18	Peço que estejam conectados para acompanhamento.
Sistema	24/11/2025 às 14:10:18	Senhores, boa tarde!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 15 horas do dia 25/11/2025 para prosseguimento do julgamento.
Sistema	25/11/2025 às 11:38:30	Senhores, bom dia!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 15 horas do dia 26/11/2025 para prosseguimento do julgamento.

Responsável	Data/Hora	Mensagem
Sistema	25/11/2025 às 11:38:42	Peço que estejam conectados para acompanhamento.
Sistema	26/11/2025 às 15:01:52	Senhores, boa tarde!!
Sistema	26/11/2025 às 15:02:08	Daremos prosseguimento ao julgamento.
Sistema	26/11/2025 às 15:15:48	Por ter atendido aos requisitos do Edital e anexos, a empresa REDES VIX LTDA será habilitada.

Eventos da compra

Data/Hora	Descrição
29/10/2025 às 09:00:04	Abertura da sessão pública
29/10/2025 às 09:39:45	Início da etapa de julgamento de propostas

Item 1 - Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC)

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

Quantidade:	1	Valor estimado:	R\$ 480.000,0000 (unitário)
Unidade de fornecimento:	UNIDADE		R\$ 480.000,0000 (total)
Intervalo mínimo entre lances:	R\$ 1.000,0000	Situação:	Aberto para recursos
Critério de julgamento:	Menor Preço		

Aceito e Habilitado por CPF ***.479.***-5 - AMYLENE SHNEIDER GONCALVES DELUNARDO para REDES VIX LTDA, CNPJ 44.447.862/0001-32, melhor lance: R\$ 289.000,0000 (unitário) / R\$ 289.000,0000 (total), valor negociado: R\$ 260.000,0400 (unitário) / R\$ 260.000,0400 (total)

Propostas do Item 1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nº 123, de 14 de dezembro de 2006
Programa de integridade: Conforme termos previstos na Lei nº 14.133/2021 e no Decreto nº 12.304/2024

Fornecedor	Valor ofertado	Situação
14.698.571/0001-56 - AT&TI SOLUCOES EM TECNOLOGIA LTDA Benefício Me/Epp: Não Programa de integridade: Sim UF endereço: ES	R\$ 340.000,0000 (unitário) R\$ 340.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
36.770.097/0001-69 - CIB EMPREENDIMENTOS IMOBILIARIOS LTDA Benefício Me/Epp: Não Programa de integridade: Sim UF endereço: MG	R\$ 495.456,0000 (unitário) R\$ 495.456,0000 (total)	-
Valor proposta: R\$ 495.456,0000 (unitário) R\$ 495.456,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
57.135.675/0001-65 - COMERCIAL LENA LTDA Benefício Me/Epp: Sim Programa de integridade: Não UF endereço: SP	R\$ 464.000,0000 (unitário) R\$ 464.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Fornecedor	Valor ofertado	Situação
10.215.066/0001-52 - FUTURA SOLUCOES NETWORKS E SERVICOS LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: MG	R\$ 465.000,0000 (unitário) R\$ 465.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
48.431.950/0001-05 - GABRIEL ALEX RAMIRO MARTINS 22834623805 Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: SP	R\$ 292.000,0000 (unitário) R\$ 292.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
37.007.414/0001-52 - INFINITY STORE COMERCIO E SERVICOS DE INFORMATICA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: RO	R\$ 390.000,0000 (unitário) R\$ 390.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
29.297.426/0001-30 - INFOMAX SOLUCOES EM TECNOLOGIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: SE	R\$ 460.000,0000 (unitário) R\$ 460.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
70.946.330/0001-50 - INFRA DO BRASIL COMERCIO E SERVICOS LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: MG	R\$ 293.000,0000 (unitário) R\$ 293.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
32.586.528/0001-80 - MA TECNOLOGIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Fornecedor	Valor ofertado	Situação
10.635.032/0001-17 - MECSAM SERVICOS DE ENGENHARIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: AM	R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)	-
Valor proposta: R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
23.936.997/0001-91 - MGDATA TECNOLOGIA LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: MG	R\$ 384.000,0000 (unitário) R\$ 384.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
15.549.061/0001-80 - PRINT SOLUCAO EM TECNOLOGIA LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: ES	R\$ 383.000,0000 (unitário) R\$ 383.000,0000 (total)	-
Valor proposta: R\$ 468.000,0000 (unitário) R\$ 468.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
44.447.862/0001-32 - REDES VIX LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 289.000,0000 (unitário) R\$ 289.000,0000 (total)	Fornecedor habilitado
Valor proposta: R\$ 444.000,0000 (unitário) R\$ 444.000,0000 (total)	Valor negociado: R\$ 260.000,0400 (unitário) R\$ 260.000,0400 (total)	Quantidade ofertada: 1
55.298.629/0001-51 - SMART FUSION TECHNOLOGY LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 310.000,0000 (unitário) R\$ 310.000,0000 (total)	-
Valor proposta: R\$ 460.000,0000 (unitário) R\$ 460.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
10.757.593/0001-99 - THS TECNOLOGIA INFORMACAO E COMUNICACAO LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: DF	R\$ 1.480.000,0000 (unitário) R\$ 1.480.000,0000 (total)	-
Valor proposta: R\$ 1.480.000,0000 (unitário) R\$ 1.480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
52.851.499/0001-44 - WINK TELECOMUNICACOES LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: AM	R\$ 304.000,0000 (unitário) R\$ 304.000,0000 (total)	-
Valor proposta: R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 1

Data/hora	Participante	Lance
29/10/2025 às 09:06:54	70.946.330/0001-50	R\$ 443.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:07:18	48.431.950/0001-05	R\$ 442.000,0000
29/10/2025 às 09:07:37	55.298.629/0001-51	R\$ 441.000,0000
29/10/2025 às 09:08:03	48.431.950/0001-05	R\$ 440.000,0000
29/10/2025 às 09:08:03	37.007.414/0001-52	R\$ 442.500,0000
29/10/2025 às 09:08:43	23.936.997/0001-91	R\$ 439.000,0000
29/10/2025 às 09:09:08	70.946.330/0001-50	R\$ 438.000,0000
29/10/2025 às 09:09:30	48.431.950/0001-05	R\$ 437.000,0000
29/10/2025 às 09:09:36	57.135.675/0001-65	R\$ 467.000,0000
29/10/2025 às 09:09:43	70.946.330/0001-50	R\$ 436.000,0000
29/10/2025 às 09:09:55	44.447.862/0001-32	R\$ 434.000,0000
29/10/2025 às 09:10:04	70.946.330/0001-50	R\$ 433.000,0000
29/10/2025 às 09:10:18	23.936.997/0001-91	R\$ 430.000,0000
29/10/2025 às 09:10:22	70.946.330/0001-50	R\$ 429.000,0000
29/10/2025 às 09:10:34	55.298.629/0001-51	R\$ 426.000,0000
29/10/2025 às 09:10:39	44.447.862/0001-32	R\$ 425.000,0000
29/10/2025 às 09:11:00	52.851.499/0001-44	R\$ 424.000,0000
29/10/2025 às 09:11:03	23.936.997/0001-91	R\$ 422.000,0000
29/10/2025 às 09:11:12	48.431.950/0001-05	R\$ 421.000,0000
29/10/2025 às 09:11:27	70.946.330/0001-50	R\$ 420.000,0000
29/10/2025 às 09:11:55	23.936.997/0001-91	R\$ 419.000,0000
29/10/2025 às 09:12:21	70.946.330/0001-50	R\$ 418.000,0000
29/10/2025 às 09:12:23	10.215.066/0001-52	R\$ 470.000,0000
29/10/2025 às 09:12:24	44.447.862/0001-32	R\$ 415.000,0000
29/10/2025 às 09:12:39	23.936.997/0001-91	R\$ 414.000,0000
29/10/2025 às 09:12:45	70.946.330/0001-50	R\$ 413.000,0000
29/10/2025 às 09:13:17	37.007.414/0001-52	R\$ 420.000,0000
29/10/2025 às 09:13:27	23.936.997/0001-91	R\$ 410.000,0000
29/10/2025 às 09:13:36	70.946.330/0001-50	R\$ 409.000,0000
29/10/2025 às 09:13:38	52.851.499/0001-44	R\$ 410.000,0000
29/10/2025 às 09:13:44	52.851.499/0001-44	R\$ 408.000,0000
29/10/2025 às 09:13:48	70.946.330/0001-50	R\$ 407.000,0000
29/10/2025 às 09:13:55	23.936.997/0001-91	R\$ 405.000,0000
29/10/2025 às 09:14:01	70.946.330/0001-50	R\$ 404.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:14:23	23.936.997/0001-91	R\$ 401.000,0000
29/10/2025 às 09:14:29	44.447.862/0001-32	R\$ 400.000,0000
29/10/2025 às 09:14:39	70.946.330/0001-50	R\$ 399.000,0000
29/10/2025 às 09:15:02	48.431.950/0001-05	R\$ 398.000,0000
29/10/2025 às 09:15:07	70.946.330/0001-50	R\$ 397.000,0000
29/10/2025 às 09:15:11	23.936.997/0001-91	R\$ 395.000,0000
29/10/2025 às 09:15:20	70.946.330/0001-50	R\$ 394.000,0000
29/10/2025 às 09:15:35	37.007.414/0001-52	R\$ 399.999,0000
29/10/2025 às 09:15:58	52.851.499/0001-44	R\$ 393.000,0000
29/10/2025 às 09:16:08	23.936.997/0001-91	R\$ 390.000,0000
29/10/2025 às 09:16:12	70.946.330/0001-50	R\$ 392.000,0000
29/10/2025 às 09:16:19	70.946.330/0001-50	R\$ 389.000,0000
29/10/2025 às 09:16:22	44.447.862/0001-32	R\$ 387.000,0000
29/10/2025 às 09:16:46	70.946.330/0001-50	R\$ 386.000,0000
29/10/2025 às 09:17:00	10.215.066/0001-52	R\$ 465.000,0000
29/10/2025 às 09:17:22	44.447.862/0001-32	R\$ 385.000,0000
29/10/2025 às 09:17:24	23.936.997/0001-91	R\$ 384.000,0000
29/10/2025 às 09:17:31	70.946.330/0001-50	R\$ 383.000,0000
29/10/2025 às 09:17:33	55.298.629/0001-51	R\$ 380.000,0000
29/10/2025 às 09:17:38	57.135.675/0001-65	R\$ 464.000,0000
29/10/2025 às 09:17:41	70.946.330/0001-50	R\$ 379.000,0000
29/10/2025 às 09:17:53	48.431.950/0001-05	R\$ 378.000,0000
29/10/2025 às 09:17:58	70.946.330/0001-50	R\$ 377.000,0000
29/10/2025 às 09:18:31	52.851.499/0001-44	R\$ 376.000,0000
29/10/2025 às 09:18:37	70.946.330/0001-50	R\$ 375.000,0000
29/10/2025 às 09:18:46	37.007.414/0001-52	R\$ 390.000,0000
29/10/2025 às 09:19:57	44.447.862/0001-32	R\$ 374.000,0000
29/10/2025 às 09:20:03	14.698.571/0001-56	R\$ 370.000,0000
29/10/2025 às 09:20:04	70.946.330/0001-50	R\$ 373.000,0000
29/10/2025 às 09:20:09	52.851.499/0001-44	R\$ 369.000,0000
29/10/2025 às 09:20:13	70.946.330/0001-50	R\$ 368.000,0000
29/10/2025 às 09:20:17	44.447.862/0001-32	R\$ 366.000,0000
29/10/2025 às 09:20:19	14.698.571/0001-56	R\$ 365.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:20:42	70.946.330/0001-50	R\$ 364.000,0000
29/10/2025 às 09:20:45	14.698.571/0001-56	R\$ 360.000,0000
29/10/2025 às 09:21:00	52.851.499/0001-44	R\$ 359.000,0000
29/10/2025 às 09:21:06	14.698.571/0001-56	R\$ 355.000,0000
29/10/2025 às 09:21:13	44.447.862/0001-32	R\$ 350.000,0000
29/10/2025 às 09:21:19	52.851.499/0001-44	R\$ 354.000,0000
29/10/2025 às 09:21:22	14.698.571/0001-56	R\$ 345.000,0000
29/10/2025 às 09:21:24	52.851.499/0001-44	R\$ 349.000,0000
29/10/2025 às 09:21:28	52.851.499/0001-44	R\$ 344.000,0000
29/10/2025 às 09:21:35	70.946.330/0001-50	R\$ 343.000,0000
29/10/2025 às 09:21:56	14.698.571/0001-56	R\$ 340.000,0000
29/10/2025 às 09:22:03	55.298.629/0001-51	R\$ 339.000,0000
29/10/2025 às 09:22:04	44.447.862/0001-32	R\$ 335.000,0000
29/10/2025 às 09:22:05	70.946.330/0001-50	R\$ 339.000,0000
29/10/2025 às 09:22:09	70.946.330/0001-50	R\$ 334.000,0000
29/10/2025 às 09:22:12	52.851.499/0001-44	R\$ 330.000,0000
29/10/2025 às 09:22:20	48.431.950/0001-05	R\$ 329.000,0000
29/10/2025 às 09:22:37	44.447.862/0001-32	R\$ 328.000,0000
29/10/2025 às 09:22:56	70.946.330/0001-50	R\$ 327.000,0000
29/10/2025 às 09:23:33	52.851.499/0001-44	R\$ 326.000,0000
29/10/2025 às 09:23:42	70.946.330/0001-50	R\$ 325.000,0000
29/10/2025 às 09:24:49	44.447.862/0001-32	R\$ 324.000,0000
29/10/2025 às 09:24:52	52.851.499/0001-44	R\$ 323.000,0000
29/10/2025 às 09:25:08	70.946.330/0001-50	R\$ 322.000,0000
29/10/2025 às 09:25:18	52.851.499/0001-44	R\$ 320.000,0000
29/10/2025 às 09:25:23	70.946.330/0001-50	R\$ 319.000,0000
29/10/2025 às 09:25:29	44.447.862/0001-32	R\$ 318.000,0000
29/10/2025 às 09:25:34	70.946.330/0001-50	R\$ 317.000,0000
29/10/2025 às 09:26:28	15.549.061/0001-80	R\$ 383.000,0000
29/10/2025 às 09:26:57	52.851.499/0001-44	R\$ 316.000,0000
29/10/2025 às 09:27:08	48.431.950/0001-05	R\$ 315.000,0000
29/10/2025 às 09:27:16	70.946.330/0001-50	R\$ 314.000,0000
29/10/2025 às 09:27:24	55.298.629/0001-51	R\$ 310.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:27:28	70.946.330/0001-50	R\$ 309.000,0000
29/10/2025 às 09:27:36	52.851.499/0001-44	R\$ 310.000,0000
29/10/2025 às 09:28:08	48.431.950/0001-05	R\$ 308.000,0000
29/10/2025 às 09:28:41	70.946.330/0001-50	R\$ 307.000,0000
29/10/2025 às 09:29:08	52.851.499/0001-44	R\$ 306.000,0000
29/10/2025 às 09:29:12	70.946.330/0001-50	R\$ 305.000,0000
29/10/2025 às 09:29:48	52.851.499/0001-44	R\$ 304.000,0000
29/10/2025 às 09:29:56	44.447.862/0001-32	R\$ 300.000,0000
29/10/2025 às 09:30:02	70.946.330/0001-50	R\$ 299.000,0000
29/10/2025 às 09:31:05	48.431.950/0001-05	R\$ 298.000,0000
29/10/2025 às 09:31:16	70.946.330/0001-50	R\$ 297.000,0000
29/10/2025 às 09:31:45	48.431.950/0001-05	R\$ 296.000,0000
29/10/2025 às 09:31:50	70.946.330/0001-50	R\$ 295.000,0000
29/10/2025 às 09:32:09	48.431.950/0001-05	R\$ 294.000,0000
29/10/2025 às 09:32:25	70.946.330/0001-50	R\$ 293.000,0000
29/10/2025 às 09:33:13	48.431.950/0001-05	R\$ 292.000,0000
29/10/2025 às 09:33:42	29.297.426/0001-30	R\$ 479.000,0000
29/10/2025 às 09:34:33	29.297.426/0001-30	R\$ 460.000,0000
29/10/2025 às 09:36:28	44.447.862/0001-32	R\$ 289.000,0000

Mensagens do chat do Item 1

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:00:04	O item 1 foi aberto. Solicitamos o envio de lances.
Sistema	29/10/2025 às 09:38:29	O item 1 está encerrado.
Sistema para o participante 44.447.862/0001-32	29/10/2025 às 09:51:50	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do Termo de Referência - anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema e siga o modelo especificado no item 12.1 do Termo de Referência, observando os valores máximos admitidos para cada subitem.
Sistema para o participante 44.447.862/0001-32	29/10/2025 às 09:53:28	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:54:00 do dia 29/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do TR - anexo do Edital. Por favor, siga o modelo especificado no item 12.1 e observe os valores máximos admitidos para cada subitem..
Pelo participante 44.447.862/0001-32	29/10/2025 às 10:27:32	O item 1 teve a convocação para envio de anexos encerrada às 10:27:32 de 29/10/2025. 5 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:03:57	Senhor Licitante, na análise da sua proposta, a área técnica demandante identificou as seguintes necessidades de ajustes:

Responsável	Data/Hora	Mensagem
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:05:30	"1. Adequação da Tabela de Preços e Valores A tabela de valores apresentada na Proposta Comercial está muito diferente do modelo e a estrutura solicitados no item 12.1 do Termo de Referência, embora dê para compreender que cada item representa os subitens solicitados no Termo de Referência, é necessário o ajuste para a correta e transparente avaliação de custos, solicitamos que a planilha de preços seja ajustada...
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:05:42	utilizando exatamente o modelo de tabela proposto no TR, garantindo a discriminação clara do valor unitário mensal de cada item e o valor total mensal e anual de cada serviço, conforme especificado no Termo de Referência.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:06:22	2. Especificação do Equipamento Controlador Wi-Fi Solicitamos também que sejam apresentados a marca e o modelo exato do Switch citado na proposta. O Equipamento deverá estar de acordo com o Termo de Referência, no item 8.1.3 ("Características do equipamento controlador de pontos de acesso Wi-Fi")."
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:07:22	Dessa forma, faremos a convocação do anexo para que a planilha de preços seja ajustada conforme modelo no Termo de Referência e a documentação solicitada pela área técnica demandante seja também encaminhada.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:09:13	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 16:10:00 do dia 30/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores, e também a documentação solicitada pela área técnica demandante e descrita no chat..
Pelo participante 44.447.862/0001-32	30/10/2025 às 14:46:32	O item 1 teve a convocação para envio de anexos encerrada às 14:46:32 de 30/10/2025. 2 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Pelo participante 44.447.862/0001-32	30/10/2025 às 14:48:30	Boa tarde, os arquivos foram alterados e enviados com sucesso. Fico à disposição para esclarecer qualquer dúvida.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:15:51	Sr. Licitante, na análise de sua proposta de preços identificamos que o subitem está com valor acima do máximo admitido no Edital, precisando ser reduzido para R\$ 3.000,00 mensais e R\$ 36.000,00 anual sem a majoração em nenhum outro subitem. Identificamos também que o valor anual do subitem 3 deverá ser de R\$ 38.000,04. Assim a proposta final deverá ser de R\$ 260.000,04.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:18:08	Faremos a convocação do anexo para o envio da proposta ajustada.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:20:21	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:20:40	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:21:00 do dia 17/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat..
Pelo participante 44.447.862/0001-32	17/11/2025 às 10:13:08	O item 1 teve a convocação para envio de anexos encerrada às 10:13:08 de 17/11/2025. 1 anexo foi enviado pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Pelo participante 44.447.862/0001-32	17/11/2025 às 10:15:56	Bom dia, Informo que a proposta foi devidamente atualizada de acordo com o que foi relatado, contemplando os ajustes mencionados nos subitens e valores anuais.
Sistema	18/11/2025 às 09:03:46	O item 1 está na etapa de julgamento de proposta no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 18/11/2025 09:13:46.
Sistema para o participante 44.447.862/0001-32	18/11/2025 às 09:18:23	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência - anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema.

Responsável	Data/Hora	Mensagem
Sistema para o participante 44.447.862/0001-32	18/11/2025 às 09:18:49	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:19:00 do dia 18/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência - anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema..
Pelo participante 44.447.862/0001-32	18/11/2025 às 10:33:56	O item 1 teve a convocação para envio de anexos encerrada às 10:33:56 de 18/11/2025. 2 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Pelo participante 44.447.862/0001-32	18/11/2025 às 10:36:08	Informo que o envio solicitado foi devidamente realizado dentro do prazo estabelecido. A documentação de habilitação, incluindo todos os certificados e o Atestado de Capacidade Técnica, foi encaminhada em dois arquivos compactados.
Pelo participante 44.447.862/0001-32	26/11/2025 às 10:44:51	Bom dia, Durante a conferência da documentação, percebi que, dos arquivos enviados, apenas dois estão disponíveis no portal. Parece ter ocorrido um problema e os demais não foram anexados. Poderia habilitar a opção de anexar arquivos para que eu possa enviar a documentação pendente?
Sistema para o participante 44.447.862/0001-32	26/11/2025 às 15:03:58	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para negociação de valor do item 1. Justificativa: Ajuste no sistema ao valor negociado no chat e formalizado na proposta assinada. .
Pelo participante 44.447.862/0001-32	26/11/2025 às 15:09:06	O item 1 teve a negociação de valor encerrada pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32. A negociação do item 1 foi aceita pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, tendo informado R\$ 260.000,0400.
Pelo participante 44.447.862/0001-32	26/11/2025 às 15:10:39	Valor atualizado conforme a última proposta assinada.
Sistema	26/11/2025 às 15:16:07	O item 1 está na etapa de habilitação de fornecedores no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 26/11/2025 15:26:07.
Sistema	26/11/2025 às 15:30:10	A fase de recurso do item 1 está aberta até 01/12/2025.

Eventos do Item 1

Data/Hora	Descrição
29/10/2025 às 09:00:04	Item aberto para lances.
29/10/2025 às 09:38:29	Item com etapa aberta encerrada.
29/10/2025 às 09:38:29	Item encerrado para lances.
29/10/2025 às 09:53:28	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:54:00 do dia 29/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do TR - anexo do Edital. Por favor, siga o modelo especificado no item 12.1 e observe os valores máximos admitidos para cada subitem..
29/10/2025 às 10:27:32	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
30/10/2025 às 14:09:13	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 16:10:00 do dia 30/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores, e também a documentação solicitada pela área técnica demandante e descrita no chat..
30/10/2025 às 14:46:32	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
17/11/2025 às 09:20:40	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:21:00 do dia 17/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat..
17/11/2025 às 10:13:08	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
18/11/2025 às 09:03:46	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 teve a proposta aceita, melhor lance: R\$ 289.000,0000. Motivo: Por ter atendido aos requisitos do Edital e anexos, a proposta da empresa REDES VIX LTDA será aceita..

Data/Hora	Descrição
18/11/2025 às 09:05:32	Fornecedor PRINT SOLUCAO EM TECNOLOGIA LTDA, CNPJ 15.549.061/0001-80 registra a intenção de recurso na fase julgamento.
18/11/2025 às 09:18:49	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:19:00 do dia 18/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência – anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema..
18/11/2025 às 10:33:56	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
26/11/2025 às 15:03:58	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para reavaliar a negociação de valor.
26/11/2025 às 15:09:06	Negociação encerrada. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 informou R\$ 260.000,0400.
26/11/2025 às 15:16:07	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 foi habilitado.
26/11/2025 às 15:19:03	Fornecedor PRINT SOLUCAO EM TECNOLOGIA LTDA, CNPJ 15.549.061/0001-80 registra a intenção de recurso na fase habilitação.
26/11/2025 às 15:30:10	Encerramento da sessão 1 de julgamento / habilitação.



CONSELHO REGIONAL DE CONTABILIDADE - ES

TERMO DE HOMOLOGAÇÃO
UASG 383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES
PREGÃO 90012/2025

Às 16:56 horas do dia 12 de dezembro do ano de 2025, após constatada a regularidade dos atos procedimentais, a autoridade competente, WALTERLENO MAIFREDE NORONHA, HOMOLOGA a adjudicação referente ao Processo nº 000048/2025-57, Pregão nº 90012/2025.

Fundamentação legal:	Lei 14.133/2021	Característica:	SISPP - Tradicional
Critério de julgamento:	Menor Preço / Maior Desconto	Modo de disputa:	Aberto
Compra emergencial:	Não	UF da UASG:	ES
Objeto da compra:	Serviços gerenciados de Tecnologia da Informação, em Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. Gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial, conforme detalhamento no Edital e anexos.		
Entrega de propostas:	De 14/10/2025 às 09:00 até 29/10/2025 às 09:00		
Abertura da sessão pública:	Dia 29/10/2025 às 09:00 (horário de Brasília)		

Mensagens do chat da compra

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:00:04	A sessão pública está aberta. Até 20 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Mantenham-se conectados.
Sistema	29/10/2025 às 09:01:28	Senhores licitantes, bom dia!!
Sistema	29/10/2025 às 09:01:43	Aberta a etapa de disputa de preços!!
Sistema	29/10/2025 às 09:01:51	Apresentem seus lances!!
Sistema	29/10/2025 às 09:02:04	O CRCES é um ótimo tomador de serviços. Tem credibilidade no mercado por sua boa administração e principalmente pelo comprometimento com a sociedade.
Sistema	29/10/2025 às 09:02:18	Prezamos, além do preço, pela qualidade. Observem as especificações do Edital e do Termo de Referência. Não vamos aceitar serviços inferiores ao especificado.
Sistema	29/10/2025 às 09:02:28	A prestação de serviços para o CRCES é um ótima referência, além da garantia do recebimento pontual, desde que cumpridos os requisitos exigidos no Termo de Referência.
Sistema	29/10/2025 às 09:04:14	Melhem seus lances para que este certame seja um sucesso.
Sistema	29/10/2025 às 09:24:52	Prezamos, além do preço, pela qualidade. Observem as especificações do Edital e do Termo de Referência. Não vamos aceitar serviços inferiores ao especificado.
Sistema	29/10/2025 às 09:39:46	A etapa de julgamento de propostas foi iniciada. Para acompanhá-la acesse a opção "Seleção de fornecedores" na linha do tempo.
Sistema	29/10/2025 às 09:39:46	Esta compra é de órgão ou entidade da esfera federal, motivo pelo qual não se aplica o critério de desempate previsto no § 1º, inciso I do Art.60 da lei 14.133/2021.
Sistema	29/10/2025 às 09:40:49	Senhores, daremos início a etapa de julgamento.
Sistema	29/10/2025 às 09:41:00	Peço que permaneçam conectados.
Sistema	29/10/2025 às 09:42:33	Convocaremos a primeira colocada.

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:57:13	Senhores, suspenderemos a sessão para que a primeira colocada possa ajustar sua proposta e enviá-la juntamente com a documentação solicitada.
Sistema	29/10/2025 às 09:57:48	Retornaremos online para prosseguimento do julgamento as 15 horas de hoje, dia 29/10/2025.
Sistema	29/10/2025 às 09:58:05	Peço que estejam conectados para acompanhamento.
Sistema	29/10/2025 às 14:07:11	Boa tarde!! Tendo em vista não ter concluído a conferência da documentação, informo que retornaremos online as 14 horas de amanhã, dia 30/10/2025, para prosseguimento do julgamento.
Sistema	29/10/2025 às 14:07:22	Peço que estejam conectados para acompanhamento.
Sistema	30/10/2025 às 14:01:15	Senhores, boa tarde!! Daremos prosseguimento ao julgamento.
Sistema	30/10/2025 às 14:09:43	Senhores, suspenderemos a sessão para que a primeira colocada possa ajustar sua proposta e enviá-la juntamente com a documentação solicitada.
Sistema	30/10/2025 às 14:10:09	Retornaremos online para prosseguimento do julgamento as 14 horas do dia 31/10/2025.
Sistema	30/10/2025 às 14:10:18	Peço que estejam conectados para acompanhamento.
Sistema	31/10/2025 às 14:09:20	Senhores, boa tarde!
Sistema	31/10/2025 às 14:09:53	O julgamento do Pregão será suspenso. Avisaremos via sistema, com no mínimo de 24 (vinte e quatro) horas úteis de antecedência, a data e hora do retorno do julgamento.
Sistema	31/10/2025 às 14:10:06	Estejam atentos as mensagens e avisos do sistema.
Sistema	13/11/2025 às 17:30:56	Senhores, boa tarde! Informo que daremos prosseguimento ao julgamento as 09 horas do dia 17/11/2025. Peço que estejam conectados para acompanhamento.
Sistema	17/11/2025 às 09:01:41	Senhores, bom dia!! Daremos prosseguimento ao julgamento.
Sistema	17/11/2025 às 09:21:48	Suspenderemos a sessão para que a empresa REDES VIX LTDA possa ajustar e enviar sua proposta de preços.
Sistema	17/11/2025 às 09:22:17	Retornaremos online às 09 horas do dia 18/11/2025 para prosseguimento do julgamento.
Sistema	17/11/2025 às 09:22:24	Peço que estejam conectados para acompanhamento.
Sistema	18/11/2025 às 09:01:57	Senhores, bom dia!! Daremos prosseguimento ao julgamento.
Sistema	18/11/2025 às 09:03:31	Por ter atendido aos requisitos do Edital e anexos, a proposta da empresa REDES VIX LTDA será aceita.
Sistema	18/11/2025 às 09:15:54	Considerando a distinção das fases no Pregão, passaremos a fase de habilitação.
Sistema	18/11/2025 às 09:19:34	Suspenderemos a sessão para que a empresa REDES VIX LTDA possa enviar sua documentação de habilitação.
Sistema	18/11/2025 às 09:20:16	Retornaremos online às 09 horas do dia 19/11/2025 para prosseguimento do julgamento.
Sistema	18/11/2025 às 09:20:33	Peço que estejam conectados para acompanhamento.
Sistema	19/11/2025 às 13:05:24	Boa tarde!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 14 horas do dia 24/11/2025 para prosseguimento do julgamento.
Sistema	19/11/2025 às 13:05:42	Peço que estejam conectados para acompanhamento.
Sistema	19/11/2025 às 13:07:18	Peço que estejam conectados para acompanhamento.
Sistema	24/11/2025 às 14:10:18	Senhores, boa tarde!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 15 horas do dia 25/11/2025 para prosseguimento do julgamento.
Sistema	25/11/2025 às 11:38:30	Senhores, bom dia!! Tendo em vista não ter sido concluída a conferência da documentação, informo que retornaremos online as 15 horas do dia 26/11/2025 para prosseguimento do julgamento.

Responsável	Data/Hora	Mensagem
Sistema	25/11/2025 às 11:38:42	Peço que estejam conectados para acompanhamento.
Sistema	26/11/2025 às 15:01:52	Senhores, boa tarde!!
Sistema	26/11/2025 às 15:02:08	Daremos prosseguimento ao julgamento.
Sistema	26/11/2025 às 15:15:48	Por ter atendido aos requisitos do Edital e anexos, a empresa REDES VIX LTDA será habilitada.

Eventos da compra

Data/Hora	Descrição
29/10/2025 às 09:00:04	Abertura da sessão pública
29/10/2025 às 09:39:45	Início da etapa de julgamento de propostas

Item 1 - Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC)

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento e seus anexos.

Quantidade:	1	Valor estimado:	R\$ 480.000,0000 (unitário)
Unidade de fornecimento:	UNIDADE		R\$ 480.000,0000 (total)
Intervalo mínimo entre lances:	R\$ 1.000,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		

Adjudicado e Homologado por CPF ***.257.***-2 - WALTERLENO MAIFREDE NORONHA para REDES VIX LTDA, CNPJ 44.447.862/0001-32, melhor lance: R\$ 289.000,0000 (unitário) / R\$ 289.000,0000 (total), valor negociado: R\$ 260.000,0400 (unitário) / R\$ 260.000,0400 (total)

Propostas do Item 1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nº 123, de 14 de dezembro de 2006

Programa de integridade: Conforme termos previstos na Lei nº 14.133/2021 e no Decreto nº 12.304/2024

Fornecedor	Valor ofertado	Situação
14.698.571/0001-56 - AT&TI SOLUCOES EM TECNOLOGIA LTDA Benefício Me/Epp: Não Programa de integridade: Sim UF endereço: ES	R\$ 340.000,0000 (unitário) R\$ 340.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
36.770.097/0001-69 - CIB EMPREENDIMENTOS IMOBILIARIOS LTDA Benefício Me/Epp: Não Programa de integridade: Sim UF endereço: MG	R\$ 495.456,0000 (unitário) R\$ 495.456,0000 (total)	-
Valor proposta: R\$ 495.456,0000 (unitário) R\$ 495.456,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
57.135.675/0001-65 - COMERCIAL LENA LTDA Benefício Me/Epp: Sim Programa de integridade: Não UF endereço: SP	R\$ 464.000,0000 (unitário) R\$ 464.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Fornecedor	Valor ofertado	Situação
10.215.066/0001-52 - FUTURA SOLUCOES NETWORKS E SERVICOS LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: MG	R\$ 465.000,0000 (unitário) R\$ 465.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
48.431.950/0001-05 - GABRIEL ALEX RAMIRO MARTINS 22834623805 Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: SP	R\$ 292.000,0000 (unitário) R\$ 292.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
37.007.414/0001-52 - INFINITY STORE COMERCIO E SERVICOS DE INFORMATICA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: RO	R\$ 390.000,0000 (unitário) R\$ 390.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
29.297.426/0001-30 - INFOMAX SOLUCOES EM TECNOLOGIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: SE	R\$ 460.000,0000 (unitário) R\$ 460.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
70.946.330/0001-50 - INFRA DO BRASIL COMERCIO E SERVICOS LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: MG	R\$ 293.000,0000 (unitário) R\$ 293.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
32.586.528/0001-80 - MA TECNOLOGIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Fornecedor	Valor ofertado		Situação
10.635.032/0001-17 - MECSAM SERVICOS DE ENGENHARIA LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: AM	R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)		-
Valor proposta: R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	
23.936.997/0001-91 - MGDATA TECNOLOGIA LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: MG	R\$ 384.000,0000 (unitário) R\$ 384.000,0000 (total)		-
Valor proposta: R\$ 480.000,0000 (unitário) R\$ 480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	
15.549.061/0001-80 - PRINT SOLUCAO EM TECNOLOGIA LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: ES	R\$ 383.000,0000 (unitário) R\$ 383.000,0000 (total)		-
Valor proposta: R\$ 468.000,0000 (unitário) R\$ 468.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	
44.447.862/0001-32 - REDES VIX LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 289.000,0000 (unitário) R\$ 289.000,0000 (total)		Proposta adjudicada
Valor proposta: R\$ 444.000,0000 (unitário) R\$ 444.000,0000 (total)	Valor negociado: R\$ 260.000,0400 (unitário) R\$ 260.000,0400 (total)	Quantidade ofertada: 1	
55.298.629/0001-51 - SMART FUSION TECHNOLOGY LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: ES	R\$ 310.000,0000 (unitário) R\$ 310.000,0000 (total)		-
Valor proposta: R\$ 460.000,0000 (unitário) R\$ 460.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	
10.757.593/0001-99 - THS TECNOLOGIA INFORMACAO E COMUNICACAO LTDA Beneficio Me/Epp: Não Programa de integridade: Sim UF endereço: DF	R\$ 1.480.000,0000 (unitário) R\$ 1.480.000,0000 (total)		-
Valor proposta: R\$ 1.480.000,0000 (unitário) R\$ 1.480.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	
52.851.499/0001-44 - WINK TELECOMUNICACOES LTDA Beneficio Me/Epp: Sim Programa de integridade: Sim UF endereço: AM	R\$ 304.000,0000 (unitário) R\$ 304.000,0000 (total)		-
Valor proposta: R\$ 475.000,0000 (unitário) R\$ 475.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1	

Lances do Item 1

Data/hora	Participante	Lance
29/10/2025 às 09:06:54	70.946.330/0001-50	R\$ 443.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:07:18	48.431.950/0001-05	R\$ 442.000,0000
29/10/2025 às 09:07:37	55.298.629/0001-51	R\$ 441.000,0000
29/10/2025 às 09:08:03	48.431.950/0001-05	R\$ 440.000,0000
29/10/2025 às 09:08:03	37.007.414/0001-52	R\$ 442.500,0000
29/10/2025 às 09:08:43	23.936.997/0001-91	R\$ 439.000,0000
29/10/2025 às 09:09:08	70.946.330/0001-50	R\$ 438.000,0000
29/10/2025 às 09:09:30	48.431.950/0001-05	R\$ 437.000,0000
29/10/2025 às 09:09:36	57.135.675/0001-65	R\$ 467.000,0000
29/10/2025 às 09:09:43	70.946.330/0001-50	R\$ 436.000,0000
29/10/2025 às 09:09:55	44.447.862/0001-32	R\$ 434.000,0000
29/10/2025 às 09:10:04	70.946.330/0001-50	R\$ 433.000,0000
29/10/2025 às 09:10:18	23.936.997/0001-91	R\$ 430.000,0000
29/10/2025 às 09:10:22	70.946.330/0001-50	R\$ 429.000,0000
29/10/2025 às 09:10:34	55.298.629/0001-51	R\$ 426.000,0000
29/10/2025 às 09:10:39	44.447.862/0001-32	R\$ 425.000,0000
29/10/2025 às 09:11:00	52.851.499/0001-44	R\$ 424.000,0000
29/10/2025 às 09:11:03	23.936.997/0001-91	R\$ 422.000,0000
29/10/2025 às 09:11:12	48.431.950/0001-05	R\$ 421.000,0000
29/10/2025 às 09:11:27	70.946.330/0001-50	R\$ 420.000,0000
29/10/2025 às 09:11:55	23.936.997/0001-91	R\$ 419.000,0000
29/10/2025 às 09:12:21	70.946.330/0001-50	R\$ 418.000,0000
29/10/2025 às 09:12:23	10.215.066/0001-52	R\$ 470.000,0000
29/10/2025 às 09:12:24	44.447.862/0001-32	R\$ 415.000,0000
29/10/2025 às 09:12:39	23.936.997/0001-91	R\$ 414.000,0000
29/10/2025 às 09:12:45	70.946.330/0001-50	R\$ 413.000,0000
29/10/2025 às 09:13:17	37.007.414/0001-52	R\$ 420.000,0000
29/10/2025 às 09:13:27	23.936.997/0001-91	R\$ 410.000,0000
29/10/2025 às 09:13:36	70.946.330/0001-50	R\$ 409.000,0000
29/10/2025 às 09:13:38	52.851.499/0001-44	R\$ 410.000,0000
29/10/2025 às 09:13:44	52.851.499/0001-44	R\$ 408.000,0000
29/10/2025 às 09:13:48	70.946.330/0001-50	R\$ 407.000,0000
29/10/2025 às 09:13:55	23.936.997/0001-91	R\$ 405.000,0000
29/10/2025 às 09:14:01	70.946.330/0001-50	R\$ 404.000,0000
29/10/2025 às 09:14:23	23.936.997/0001-91	R\$ 401.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:14:29	44.447.862/0001-32	R\$ 400.000,0000
29/10/2025 às 09:14:39	70.946.330/0001-50	R\$ 399.000,0000
29/10/2025 às 09:15:02	48.431.950/0001-05	R\$ 398.000,0000
29/10/2025 às 09:15:07	70.946.330/0001-50	R\$ 397.000,0000
29/10/2025 às 09:15:11	23.936.997/0001-91	R\$ 395.000,0000
29/10/2025 às 09:15:20	70.946.330/0001-50	R\$ 394.000,0000
29/10/2025 às 09:15:35	37.007.414/0001-52	R\$ 399.999,0000
29/10/2025 às 09:15:58	52.851.499/0001-44	R\$ 393.000,0000
29/10/2025 às 09:16:08	23.936.997/0001-91	R\$ 390.000,0000
29/10/2025 às 09:16:12	70.946.330/0001-50	R\$ 392.000,0000
29/10/2025 às 09:16:19	70.946.330/0001-50	R\$ 389.000,0000
29/10/2025 às 09:16:22	44.447.862/0001-32	R\$ 387.000,0000
29/10/2025 às 09:16:46	70.946.330/0001-50	R\$ 386.000,0000
29/10/2025 às 09:17:00	10.215.066/0001-52	R\$ 465.000,0000
29/10/2025 às 09:17:22	44.447.862/0001-32	R\$ 385.000,0000
29/10/2025 às 09:17:24	23.936.997/0001-91	R\$ 384.000,0000
29/10/2025 às 09:17:31	70.946.330/0001-50	R\$ 383.000,0000
29/10/2025 às 09:17:33	55.298.629/0001-51	R\$ 380.000,0000
29/10/2025 às 09:17:38	57.135.675/0001-65	R\$ 464.000,0000
29/10/2025 às 09:17:41	70.946.330/0001-50	R\$ 379.000,0000
29/10/2025 às 09:17:53	48.431.950/0001-05	R\$ 378.000,0000
29/10/2025 às 09:17:58	70.946.330/0001-50	R\$ 377.000,0000
29/10/2025 às 09:18:31	52.851.499/0001-44	R\$ 376.000,0000
29/10/2025 às 09:18:37	70.946.330/0001-50	R\$ 375.000,0000
29/10/2025 às 09:18:46	37.007.414/0001-52	R\$ 390.000,0000
29/10/2025 às 09:19:57	44.447.862/0001-32	R\$ 374.000,0000
29/10/2025 às 09:20:03	14.698.571/0001-56	R\$ 370.000,0000
29/10/2025 às 09:20:04	70.946.330/0001-50	R\$ 373.000,0000
29/10/2025 às 09:20:09	52.851.499/0001-44	R\$ 369.000,0000
29/10/2025 às 09:20:13	70.946.330/0001-50	R\$ 368.000,0000
29/10/2025 às 09:20:17	44.447.862/0001-32	R\$ 366.000,0000
29/10/2025 às 09:20:19	14.698.571/0001-56	R\$ 365.000,0000
29/10/2025 às 09:20:42	70.946.330/0001-50	R\$ 364.000,0000
29/10/2025 às 09:20:45	14.698.571/0001-56	R\$ 360.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:21:00	52.851.499/0001-44	R\$ 359.000,0000
29/10/2025 às 09:21:06	14.698.571/0001-56	R\$ 355.000,0000
29/10/2025 às 09:21:13	44.447.862/0001-32	R\$ 350.000,0000
29/10/2025 às 09:21:19	52.851.499/0001-44	R\$ 354.000,0000
29/10/2025 às 09:21:22	14.698.571/0001-56	R\$ 345.000,0000
29/10/2025 às 09:21:24	52.851.499/0001-44	R\$ 349.000,0000
29/10/2025 às 09:21:28	52.851.499/0001-44	R\$ 344.000,0000
29/10/2025 às 09:21:35	70.946.330/0001-50	R\$ 343.000,0000
29/10/2025 às 09:21:56	14.698.571/0001-56	R\$ 340.000,0000
29/10/2025 às 09:22:03	55.298.629/0001-51	R\$ 339.000,0000
29/10/2025 às 09:22:04	44.447.862/0001-32	R\$ 335.000,0000
29/10/2025 às 09:22:05	70.946.330/0001-50	R\$ 339.000,0000
29/10/2025 às 09:22:09	70.946.330/0001-50	R\$ 334.000,0000
29/10/2025 às 09:22:12	52.851.499/0001-44	R\$ 330.000,0000
29/10/2025 às 09:22:20	48.431.950/0001-05	R\$ 329.000,0000
29/10/2025 às 09:22:37	44.447.862/0001-32	R\$ 328.000,0000
29/10/2025 às 09:22:56	70.946.330/0001-50	R\$ 327.000,0000
29/10/2025 às 09:23:33	52.851.499/0001-44	R\$ 326.000,0000
29/10/2025 às 09:23:42	70.946.330/0001-50	R\$ 325.000,0000
29/10/2025 às 09:24:49	44.447.862/0001-32	R\$ 324.000,0000
29/10/2025 às 09:24:52	52.851.499/0001-44	R\$ 323.000,0000
29/10/2025 às 09:25:08	70.946.330/0001-50	R\$ 322.000,0000
29/10/2025 às 09:25:18	52.851.499/0001-44	R\$ 320.000,0000
29/10/2025 às 09:25:23	70.946.330/0001-50	R\$ 319.000,0000
29/10/2025 às 09:25:29	44.447.862/0001-32	R\$ 318.000,0000
29/10/2025 às 09:25:34	70.946.330/0001-50	R\$ 317.000,0000
29/10/2025 às 09:26:28	15.549.061/0001-80	R\$ 383.000,0000
29/10/2025 às 09:26:57	52.851.499/0001-44	R\$ 316.000,0000
29/10/2025 às 09:27:08	48.431.950/0001-05	R\$ 315.000,0000
29/10/2025 às 09:27:16	70.946.330/0001-50	R\$ 314.000,0000
29/10/2025 às 09:27:24	55.298.629/0001-51	R\$ 310.000,0000
29/10/2025 às 09:27:28	70.946.330/0001-50	R\$ 309.000,0000
29/10/2025 às 09:27:36	52.851.499/0001-44	R\$ 310.000,0000
29/10/2025 às 09:28:08	48.431.950/0001-05	R\$ 308.000,0000

Data/hora	Participante	Lance
29/10/2025 às 09:28:41	70.946.330/0001-50	R\$ 307.000,0000
29/10/2025 às 09:29:08	52.851.499/0001-44	R\$ 306.000,0000
29/10/2025 às 09:29:12	70.946.330/0001-50	R\$ 305.000,0000
29/10/2025 às 09:29:48	52.851.499/0001-44	R\$ 304.000,0000
29/10/2025 às 09:29:56	44.447.862/0001-32	R\$ 300.000,0000
29/10/2025 às 09:30:02	70.946.330/0001-50	R\$ 299.000,0000
29/10/2025 às 09:31:05	48.431.950/0001-05	R\$ 298.000,0000
29/10/2025 às 09:31:16	70.946.330/0001-50	R\$ 297.000,0000
29/10/2025 às 09:31:45	48.431.950/0001-05	R\$ 296.000,0000
29/10/2025 às 09:31:50	70.946.330/0001-50	R\$ 295.000,0000
29/10/2025 às 09:32:09	48.431.950/0001-05	R\$ 294.000,0000
29/10/2025 às 09:32:25	70.946.330/0001-50	R\$ 293.000,0000
29/10/2025 às 09:33:13	48.431.950/0001-05	R\$ 292.000,0000
29/10/2025 às 09:33:42	29.297.426/0001-30	R\$ 479.000,0000
29/10/2025 às 09:34:33	29.297.426/0001-30	R\$ 460.000,0000
29/10/2025 às 09:36:28	44.447.862/0001-32	R\$ 289.000,0000

Mensagens do chat do Item 1

Responsável	Data/Hora	Mensagem
Sistema	29/10/2025 às 09:00:04	O item 1 foi aberto. Solicitamos o envio de lances.
Sistema	29/10/2025 às 09:38:29	O item 1 está encerrado.
Sistema para o participante 44.447.862/0001-32	29/10/2025 às 09:51:50	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do Termo de Referência – anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema e siga o modelo especificado no item 12.1 do Termo de Referência, observando os valores máximos admitidos para cada subitem.
Sistema para o participante 44.447.862/0001-32	29/10/2025 às 09:53:28	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:54:00 do dia 29/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do TR – anexo do Edital. Por favor, siga o modelo especificado no item 12.1 e observe os valores máximos admitidos para cada subitem..
Pelo participante 44.447.862/0001-32	29/10/2025 às 10:27:32	O item 1 teve a convocação para envio de anexos encerrada às 10:27:32 de 29/10/2025. 5 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:03:57	Senhor Licitante, na análise da sua proposta, a área técnica demandante identificou as seguintes necessidades de ajustes:
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:05:30	"1. Adequação da Tabela de Preços e Valores A tabela de valores apresentada na Proposta Comercial está muito diferente do modelo e a estrutura solicitados no item 12.1 do Termo de Referência, embora dê para compreender que cada item representa os subitens solicitados no Termo de Referência, é necessário o ajuste para a correta e transparente avaliação de custos, solicitamos que a planilha de preços seja ajustada...

Responsável	Data/Hora	Mensagem
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:05:42	utilizando exatamente o modelo de tabela proposto no TR, garantindo a discriminação clara do valor unitário mensal de cada item e o valor total mensal e anual de cada serviço, conforme especificado no Termo de Referência.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:06:22	2. Especificação do Equipamento Controlador Wi-Fi Solicitamos também que sejam apresentados a marca e o modelo exato do Switch citado na proposta. O Equipamento deverá estar de acordo com o Termo de Referência, no item 8.1.3 ("Características do equipamento controlador de pontos de acesso Wi-Fi")."
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:07:22	Dessa forma, faremos a convocação do anexo para que a planilha de preços seja ajustada conforme modelo no Termo de Referência e a documentação solicitada pela área técnica demandante seja também encaminhada.
Sistema para o participante 44.447.862/0001-32	30/10/2025 às 14:09:13	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 16:10:00 do dia 30/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores, e também a documentação solicitada pela área técnica demandante e descrita no chat..
Pelo participante 44.447.862/0001-32	30/10/2025 às 14:46:32	O item 1 teve a convocação para envio de anexos encerrada às 14:46:32 de 30/10/2025. 2 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Pelo participante 44.447.862/0001-32	30/10/2025 às 14:48:30	Boa tarde, os arquivos foram alterados e enviados com sucesso. Fico à disposição para esclarecer qualquer dúvida.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:15:51	Sr. Licitante, na análise de sua proposta de preços identificamos que o subitem está com valor acima do máximo admitido no Edital, precisando ser reduzido para R\$ 3.000,00 mensais e R\$ 36.000,00 anual sem a majoração em nenhum outro subitem. Identificamos também que o valor anual do subitem 3 deverá ser de R\$ 38.000,04. Assim a proposta final deverá ser de R\$ 260.000,04.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:18:08	Faremos a convocação do anexo para o envio da proposta ajustada.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:20:21	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat.
Sistema para o participante 44.447.862/0001-32	17/11/2025 às 09:20:40	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:21:00 do dia 17/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência - anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat..
Pelo participante 44.447.862/0001-32	17/11/2025 às 10:13:08	O item 1 teve a convocação para envio de anexos encerrada às 10:13:08 de 17/11/2025. 1 anexo foi enviado pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.
Pelo participante 44.447.862/0001-32	17/11/2025 às 10:15:56	Bom dia, Informo que a proposta foi devidamente atualizada de acordo com o que foi relatado, contemplando os ajustes mencionados nos subitens e valores anuais.
Sistema	18/11/2025 às 09:03:46	O item 1 está na etapa de julgamento de proposta no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 18/11/2025 09:13:46.
Sistema para o participante 44.447.862/0001-32	18/11/2025 às 09:18:23	Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência - anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema.
Sistema para o participante 44.447.862/0001-32	18/11/2025 às 09:18:49	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para enviar anexos para o item 1. Prazo para encerrar o envio: 11:19:00 do dia 18/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência - anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema..
Pelo participante 44.447.862/0001-32	18/11/2025 às 10:33:56	O item 1 teve a convocação para envio de anexos encerrada às 10:33:56 de 18/11/2025. 2 anexos foram enviados pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32.

Responsável	Data/Hora	Mensagem
Pelo participante 44.447.862/0001-32	18/11/2025 às 10:36:08	Informo que o envio solicitado foi devidamente realizado dentro do prazo estabelecido. A documentação de habilitação, incluindo todos os certificados e o Atestado de Capacidade Técnica, foi encaminhada em dois arquivos compactados.
Pelo participante 44.447.862/0001-32	26/11/2025 às 10:44:51	Bom dia, Durante a conferência da documentação, percebi que, dos arquivos enviados, apenas dois estão disponíveis no portal. Parece ter ocorrido um problema e os demais não foram anexados. Poderia habilitar a opção de anexar arquivos para que eu possa enviar a documentação pendente?
Sistema para o participante 44.447.862/0001-32	26/11/2025 às 15:03:58	Sr. Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, você foi convocado para negociação de valor do item 1. Justificativa: Ajuste no sistema ao valor negociado no chat e formalizado na proposta assinada. .
Pelo participante 44.447.862/0001-32	26/11/2025 às 15:09:06	O item 1 teve a negociação de valor encerrada pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32. A negociação do item 1 foi aceita pelo fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32, tendo informado R\$ 260.000,0400.
Pelo participante 44.447.862/0001-32	26/11/2025 às 15:10:39	Valor atualizado conforme a última proposta assinada.
Sistema	26/11/2025 às 15:16:07	O item 1 está na etapa de habilitação de fornecedores no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 26/11/2025 15:26:07.
Sistema	26/11/2025 às 15:30:10	A fase de recurso do item 1 está aberta até 01/12/2025.
Sistema	02/12/2025 às 00:00:04	A fase de recurso do item 1 foi finalizada no prazo previsto. O item está aberto para registro de contrarrazão até 04/12/2025.
Sistema	05/12/2025 às 00:00:04	A fase de contrarrazão do item 1 foi finalizada no prazo previsto. O item está aberto para decisão do pregoeiro.

Eventos do Item 1

Data/Hora	Descrição
29/10/2025 às 09:53:28	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:54:00 do dia 29/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 horas, envie A PROPOSTA DE PREÇOS ajustada ao seu último lance juntamente com a documentação descrita no item 12.2 do TR – anexo do Edital. Por favor, siga o modelo especificado no item 12.1 e observe os valores máximos admitidos para cada subitem..
29/10/2025 às 10:27:32	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
30/10/2025 às 14:09:13	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 16:10:00 do dia 30/10/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência – anexo do Edital, sem a majoração dos valores, e também a documentação solicitada pela área técnica demandante e descrita no chat..
30/10/2025 às 14:46:32	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
17/11/2025 às 09:20:40	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:21:00 do dia 17/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A PROPOSTA DE PREÇOS ajustada conforme modelo no item 12.1 do Termo de Referência – anexo do Edital, sem a majoração dos valores em outros subitens, conforme detalhamento descrito no chat..
17/11/2025 às 10:13:08	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
18/11/2025 às 09:18:49	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 convocado para o envio de anexo. Prazo para encerrar o envio: 11:19:00 do dia 18/11/2025. Justificativa: Sr. Licitante, solicito que, no prazo de 2 (duas) horas, envie A DOCUMENTAÇÃO DE HABILITAÇÃO, descrita no item 11 do Termo de Referência – anexo do Edital. Por favor, utilize a opção de enviar anexo do sistema..
18/11/2025 às 10:33:56	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 finalizou o envio de anexo.
02/12/2025 às 00:00:04	Fornecedor PRINT SOLUCAO EM TECNOLOGIA LTDA, CNPJ 15.549.061/0001-80 registra recurso.
04/12/2025 às 19:28:05	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 registra contrarrazão ao recurso do fornecedor 15.549.061/0001-80.

Data/Hora	Descrição
12/12/2025 às 16:29:03	Agente de contratação registra a decisão para os recursos cadastrados.
12/12/2025 às 16:54:51	Autoridade competente registra a revisão da decisão para os recursos cadastrados.
12/12/2025 às 16:56:17	Fornecedor REDES VIX LTDA, CNPJ 44.447.862/0001-32 teve a proposta adjudicada, melhor lance: R\$ 289.000,0000, valor negociado: R\$ 260.000,0400.
12/12/2025 às 16:56:17	Item homologado.

Fase Recursal do Item/Grupo *

* Maiores detalhes sobre recursos, contrarrazões, decisões e revisões deverão ser consultados no sistema.

Sessão 1

Prazos:	
Intenção de recurso no julgamento:	18/11/2025 09:13:46
Intenção de recurso na habilitação:	26/11/2025 15:26:07
Recurso:	01/12/2025 23:59:59
Contrarrazão:	04/12/2025 23:59:59

Recursos realizados:	
15.549.061/0001-80 - PRINT SOLUCAO EM TECNOLOGIA LTDA	
Intenção de recurso no julgamento:	18/11/2025 09:05:32
Intenção de recurso na habilitação:	26/11/2025 15:19:03
Recurso:	(Cadastrado) 01/12/2025 17:18:59
Contrarrazões:	
44.447.862/0001-32 - REDES VIX LTDA	(Cadastrado) 04/12/2025 19:28:05
Decisão do agente de contratação:	(Não procede) 12/12/2025 16:29:03
Revisão da autoridade competente:	(Mantida decisão não procede) 12/12/2025 16:54:51

CONTRATO

Processo Administrativo nº 9079618110000798.000048/2025-57

CONTRATO ADMINISTRATIVO Nº 49/2025, QUE
FAZEM ENTRE SI O CRCES E A EMPRESA REDES
VIX LTDA.

O CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO – CRCES, Autarquia Federal de Regime Especial, inscrito no CNPJ – sob o n.º 28.163.343/0001-96, com sede à Rua Amélia da Cunha Ornelas, nº 30, Bento Ferreira, Vitória/ES, CEP: 29.050- 620, representado pelo seu Presidente, o Contador WALTERLENO MAIFREDE NORONHA, nomeado pela Ata nº 1.664, de 02 de janeiro de 2024, doravante denominado CONTRATANTE, e a empresa REDES VIX LTDA, inscrita no CNPJ sob o nº 44.447.862/0001-32, sediada na Rua Pedro Palácios, nº 104, sala 701 Edifício Heitor Lugon, Centro, em Vitória/ES CEP: 29.015-160, doravante designado CONTRATADO, neste ato representada por seu Sócio Administrador ERMELINDO FERNANDES CARNEIRO, conforme atos constitutivos da empresa, tendo em vista o que consta no Processo nº 9079618110000798.000048/2025-57 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. 90012/2025, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO ([art. 92, I e II](#))

1.1. O objeto do presente instrumento é contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.

ITEM 1			
SUBITEM	ESPECIFICAÇÃO	VALOR MENSAL	VALOR ANUAL

1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	R\$ 7.500,00	R\$ 90.000,00
2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	R\$ 3.000,00	R\$ 36.000,00
3	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	R\$ 3.166,67	R\$ 38.000,04
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	R\$ 8.000,00	R\$ 96.000,00
VALOR TOTAL		R\$ 21.666,67	R\$ 260.000,04

1.2. Vinculam esta contratação, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. O Edital da Licitação;

1.2.3. A Proposta do contratado;

1.2.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses e inicia em 12/01/2026, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

- a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;
- b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;
- c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;
- d) Haja manifestação expressa do contratado informando o interesse na prorrogação;
- e) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS ([art. 92, IV, VII e XVIII](#))

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA – PREÇO ([art. 92, V](#))

5.1. O valor mensal da contratação é de R\$ R\$ 21.666,67 (vinte e um mil seiscentos e sessenta e seis reais e sessenta e sete centavos), perfazendo o valor anual de R\$ 260.000,04 (duzentos e sessenta mil reais e quatro centavos).

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – CRITÉRIOS DE PAGAMENTO E MEDIÇÃO ([art. 92, V e VI](#))

6.1 O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

6.2 No caso de atraso de pagamento(s) pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente pelo Índice IPCA - Índice de Preços ao Consumidor Amplo,

bem como incidirão juros moratórios, à razão de 0,5% (meio por cento) ao mês, aplicando-se a fórmula constante em item 5 do Anexo XI da Instrução Normativa nº 05, de 26 de maio de 2017.

7. CLÁUSULA SÉTIMA - REAJUSTE ([art. 92, V](#))

7.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, em 15/08/2025.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IPCA - Índice de Preços ao Consumidor Amplo (acumulado nos últimos 12 meses desde a apresentação da proposta), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.4. No caso de atraso ou não divulgação do índice de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

7.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

7.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE ([art. 92, X, XI e XIV](#))

8.1. São obrigações do Contratante:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

- 8.9. Cientificar o Setor Jurídico do CRCES para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;
- 8.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
- 8.10.1. A Administração terá o prazo de 05 (cinco) dias úteis, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
- 8.11. Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.
- 8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro, bem como de repactuação de preços, feitos pelo contratado no prazo máximo de 30 dias.
- 8.13. Comunicar ao Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.
- 8.15. Demais obrigações descritas no Termo de Referência.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO ([art. 92, XIV, XVI e XVII](#))

- 9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:
- 9.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior ([art. 137, II](#)) e prestar todo esclarecimento ou informação por eles solicitados;
- 9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 9.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o [Código de Defesa do Consumidor \(Lei nº 8.078, de 1990\)](#), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;
- 9.5. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do [artigo 48, parágrafo único, da Lei nº 14.133, de 2021](#);
- 9.6. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, bem como aos documentos relativos à execução do objeto.
- 9.7. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 9.8. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças na execução do objeto.

- 9.9. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 9.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- 9.11. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116](#));
- 9.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único](#));
- 9.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 9.14. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no [art. 124, II, d, da Lei nº 14.133, de 2021](#);
- 9.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;
- 9.16. Demais obrigações descritas no Termo de Referência.

10. CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

- 10.1. As partes deverão cumprir a [Lei nº 13.709, de 14 de agosto de 2018 \(LGPD\)](#), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
- 10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do [art. 6º da LGPD](#).
- 10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.
- 10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.
- 10.5. Terminado o tratamento dos dados nos termos do [art. 15 da LGPD](#), é dever do contratado eliminá-los, com exceção das hipóteses do [art. 16 da LGPD](#), incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.
- 10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
- 10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados ([LGPD, art. 37](#)), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.12. Os contratos e convênios de que trata o [§ 1º do art. 26 da LGPD](#) deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO ([art. 92, XII](#))

11.1. Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS ([art. 92, XIV](#))

12.1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2 Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

12.3 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

12.4 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

12.5 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

12.6 Multa:

12.6.1 Moratória, para as infrações descritas no item “d”, de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (sessenta) dias [\[A1\]](#) [\[A2\]](#), observados os limites previstos no §3º do art. 156.

12.6.2 Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia; [\[A3\]](#)

12.6.3 O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

12.6.4 Compensatória, para as infrações descritas acima nas alíneas “e” a “h” de 0,5% (cinco décimos por cento) a [\[A4\]](#) 30% (trinta por cento) do valor da contratação.

12.6.5 Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.6 Compensatória, para a infração descrita acima na alínea “b”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.7 Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.8 Compensatória, para a infração descrita acima na alínea “a”, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor da contratação.

12.6.9 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

12.6.10 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

12.6.11 Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.6.12 Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

12.6.13 A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.6.14 A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6.15 Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

12.6.16 Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicaf serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

12.6.17 Na aplicação das sanções serão considerados os elementos previstos no §1º do art. 156.

12.6.18 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

12.6.19 A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

12.6.20 O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

12.6.21 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

12.6.22 Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/21](#), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.1.1. Nesta hipótese, aplicam-se também os [artigos 138 e 139](#) da mesma Lei.

13.1.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.1.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.2. O termo de extinção, sempre que possível, será precedido:

13.2.1.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.2.1.2. Relação dos pagamentos já efetuados e ainda devidos;

13.2.1.3. Indenizações e multas.

13.3. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131, caput, da Lei n.º 14.133, de 2021](#)).

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA ([art. 92, VIII](#))

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES, na dotação abaixo discriminada:

6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS ([art. 92, III](#))

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na [Lei nº 14.133, de 2021](#), e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês ([art. 132 da Lei nº 14.133, de 2021](#)).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao [art. 91, caput, da Lei n.º 14.133, de 2021](#), e ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

18. CLÁUSULA DÉCIMA OITAVA– FORO (art. 92, §1º)

18.1. Fica eleito o foro da Justiça Federal de Vitória – Seção Judiciária do Espírito Santo para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme [art. 92, §1º, da Lei nº 14.133/21.](#)

Vitória/ES, 17 de dezembro de 2025.

WALTERLENO MAIFREDE NORONHA

Presidente do CRCES

Documento assinado digitalmente



ERMELINDO FERNANDES CARNEIRO

Data: 17/12/2025 13:14:12-0300

Verifique em <https://validar.it.gov.br>

ERMELINDO FERNANDES CARNEIRO

Sócio Administrador

REDES VIX LTDA

Assinado por
WALTERLENO MAIFREDE
NORONHA [REDACTED]
Data: 18/12/2025 10:43:39
+00:00

Contrato nº 49/2025

Última atualização 18/12/2025

Local: Vitória/ES **Órgão:** CONSELHO REGIONAL DE CONTABILIDADE DO ESPIRITO SANTO

Unidade executora: 383506 - CONSELHO REGIONAL DE CONTABILIDADE-ES

Tipo: Contrato (termo inicial) **Receita ou Despesa:** Despesa **Processo:** 9079618110000798.000048/2025-57

Categoria do processo: Serviços

Data de divulgação no PNCP: 18/12/2025 **Data de assinatura:** 17/12/2025 **Vigência:** de 12/01/2026 a 11/01/2027

Id contrato PNCP: 28163343000196-2-000053/2025 **Fonte:** Compras.gov.br

Id contratação PNCP: [28163343000196-1-000052/2025](#)

Objeto:

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura... [Continuar Lendo >](#)

VALOR CONTRATADO

R\$ 260.000,04

FORNECEDOR:

Tipo: Pessoa jurídica **CNPJ/CPF:** 44.447.862/0001-32 [Consultar sanções e penalidades do fornecedor](#)

Nome/Razão social: REDES VIX LTDA

Arquivos

Histórico

Nome	Data/Hora de Inclusão	Tipo
ContratoGERENCIAMENTO.pdf	18/12/2025 - 10:53:19	Contrato

Exibir: 5

1-1 de 1 itens

Página: 1

< >

< Voltar



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.

É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correteude das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portaldeservicos.gestao.gov.br>

☎ [0800 978 9001](tel:08009789001)

AGRADECIMENTO AOS PARCEIROS



Texto destinado a exibição de informações relacionadas à **licença de uso**.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

À Assessoria de Contratações
Senhora Maria Eduarda Storch,

Tendo em vista a homologação do Pregão Eletrônico nº 90012/2025, encaminho o processo para emissão da ordem de serviços, gestão e fiscalização do contrato.

Consta nos autos, a publicação do contrato no PNCP, devendo ainda ser realizada a publicação no site do CRCES.

Considerando a data do início da vigência do contrato em 12/01/2026 e a informação da área requisitante de que a execução é prevista para 2026, é necessário solicitar a emissão da nota de empenho imediatamente após a abertura do exercício 2026 e só emitir a ordem de serviços após a emissão do empenho.



Documento assinado eletronicamente por **Amylene Shneider Gonçalves Delunardo, Assistente**, em 18/12/2025, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1170918** e o código CRC **A640F762**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1170918

CRCES - Amylene Delunardo

De: CRCES - Amylene Delunardo
Enviado em: quinta-feira, 18 de dezembro de 2025 11:12
Para: 'ermelindo@redes.vix.br'
Cc: CRCES - Administrativo; CRCES - Compras
Assunto: RES: Encaminha contrato para assinatura - Pregão Eletrônico nº 90012/2025
Anexos: Contrato_GERENCIAMENTO_assinado.pdf

Prezados Senhores, bom dia!

Agradecemos o retorno.

Encaminhamos o contrato assinado pelo CRCES e ratificamos a informação de que a execução está prevista para o ano de 2026.

Dessa forma, a emissão da ordem de serviços e o início da execução do contrato somente poderão ocorrer após a abertura do orçamento 2026 e emissão da nota de empenho.

Aproveito a oportunidade e encaminho os dados da Coordenadora do Setor Administrativo, responsável pela área de TI do CRCES:

Sra Elaine Leopodino

Ramal/whatsapp: (27) 3232-1648

E-mail: administrativo@crc-es.org.br

Atenciosamente



Amylene Shneider G. Delunardo

Agente de Contratação - Portaria nº 027/2023

Licitações - CRCES

www.crc-es.org.br|licitacao@crc-es.org.br| 55 (27) 3232-1624

☐ Rua Amélia da Cunha Ornelas, Número 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

☐ Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

De: ermelindo@redes.vix.br [mailto:ermelindo@redes.vix.br]

Enviada em: quarta-feira, 17 de dezembro de 2025 13:16

Para: CRCES - Amylene Delunardo

Assunto: RES: Encaminha contrato para assinatura - Pregão Eletrônico nº 90012/2025

Boa tarde,

Confirmo que o contrato foi devidamente assinado e estou muito feliz que tudo deu certo. Estou ansioso para iniciar e realizar um excelente trabalho, garantindo a qualidade e o cumprimento de todas as etapas. Permaneço à disposição para qualquer orientação adicional.

Atenciosamente,



De: CRCES - Amylene Delunardo <amylene.delunardo@crc-es.org.br>

Enviada em: quarta-feira, 17 de dezembro de 2025 10:24

Para: ermelindo@redes.vix.br

Assunto: Encaminha contrato para assinatura - Pregão Eletrônico nº 90012/2025

Bom dia!

Prezados Senhores,

Tendo em vista a homologação do Pregão Eletrônico nº 90012/2025, segue anexo o contrato para assinatura.

Ratificamos que a assinatura poderá ser digital, desde que seja possível a confirmação de sua autenticidade.

A prestação de serviços somente poderá ser iniciada após a emissão do empenho no orçamento CRCES 2026 e a emissão da ordem de serviços.

Atenciosamente



Amylene Shneider G. Delunardo

Agente de Contratação - Portaria nº 027/2023

Licitações - CRCES

www.crc-es.org.br/licitacao@crc-es.org.br 55 (27) 3232-1624

Rua Amélia da Cunha Ornelas, Número 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

DESPACHO

Processo nº 9079618110000798.000048/2025-57

Ao Setor de Contabilidade

Solicito a emissão de nota de empenho orçamentário no valor de **R\$ 251.333,51** (duzentos e cinquenta e um mil trezentos e trinta e três reais e cinquenta e um centavos), destinada à contratação de serviços gerenciados de Tecnologia da Informação junto à empresa **Redes Vix Ltda**, referente ao **Contrato nº 49/2025**, a ser onerada na seguinte dotação orçamentária:

n.º 6.3.1.3.02.01.005 - Serviço de Tecnologia da Informação

Vigência a partir de 12/01/2026 até 31/12/2026.

Valor Mensal	Valor Diário	Valor Diário (18 dias)	Valor Mensal (11 meses)	Valor Total
R\$ 21.666,67	R\$ 722,23	R\$ 13.000,14	R\$ 238.333,37	R\$ 251.333,51



Documento assinado eletronicamente por **Maria Eduarda Storch Magalhães, Assessora**, em 05/01/2026, às 15:56, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1180173** e o código CRC **C37B328A**.

CONSELHO REGIONAL DE CONTABILIDADE DO E S
Sistema de Controle Orçamentário
NOTA DE EMPENHO

Data : 12.01.2026
Hora : 23:12

Nº Empenho	Data do Empenho	Tipo do Empenho	Processo	Nº. Reserva	Exercício
67	12.01.2026	GLOBAL	2025-57	68	2026

Conta de Despesa	Descrição da Conta	Projeto	SubProjeto
6.3.1.3.02.01.005	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO	5002 - TECNOLOGIA DA INFORMAÇÃO	-

Número do Evento	Descrição do Evento
1130	CONTRATAÇÃO DE SERVIÇOS DE INFORMÁTICA

Dados da Modalidade (Fundamentação Legal)			
Modalidade	Complemento	Número	Núm. Controle
Pregão Eletrônico		90012/2025	0

Favorecido			
Favorecido : 3578 - ERMELINDO FERNANDES CARNEIRO 09788238777		CNPJ / CPF : 44.447.862/0001-32	
Endereço : AV AUGUSTO EMILIO ESTELITA LINS		Bairro : JARDIM CAMBURI	
CEP : 29090-590	Cidade : VITORIA	UF : ES	
Banco :	Agência :	Conta :	

Histórico do Empenho	Qtde Parcelas	Valor Unitário	Valor Total Empenhado
SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO.	999	251.333,51	251.333,51

Valor por Extenso			
Duzentos e Cinquenta e Um Mil, Trezentos e Trinta e Três Reais e Cinquenta e Um Centavos			

Dotação Orçamentária	Empenhos Acumulados	Valor deste Empenho	Saldo Atual
458.674,77	55.515,05	251.333,51	151.826,21

Parcelas Executadas	Total Executado	Total a Executar	Finalizado
---	0,00	251.333,51	NAO

VITÓRIA, 12 de Janeiro de 2026

Este documento foi assinado eletronicamente com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Signatários e datas conforme horário oficial de Brasília:

✓ ANA CAROLINA DA SILVA GRILO SANTOS (CPF [REDACTED]) em 14/01/2026 14:30:06

Assinado por
WALTERLENO MAIFREDE
NORONHA [REDACTED]
Data: 14/01/2026 18:16:47
+00:00



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

Processo nº 9079618110000798.000048/2025-57

1. IDENTIFICAÇÃO

Nº da OS:	01/2026
Data de Emissão:	14/01/2026
Área Requisitante:	TECNOLOGIA DA INFORMAÇÃO
Contratante:	CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
CNPJ:	28.163.343/0001-96
Endereço:	RUA AMÉLIA DA CUNHA ORNELAS, N.º 30, BENTO FERREIRA, VITÓRIA, ES, CEP: 29.050-620
Contratada:	REDES VIX LTDA
Empenho nº:	67/2026
Contrato nº:	49/2025

2. ESPECIFICAÇÃO DOS PRODUTOS

Subitem	Descrição	Valor Mensal	Valor Anual
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	R\$ 7.500,00	R\$ 90.000,00
2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	R\$ 3.000,00	R\$ 36.000,00
3	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	R\$ 3.166,67	R\$ 38.000,04
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	R\$ 8.000,00	R\$ 96.000,00
		R\$ 21.666,67	R\$ 260.000,04

3. INSTRUÇÕES COMPLEMENTARES

3.1. Todo detalhamento das especificações, prazos e demais informações encontram-se no Termo de Referência.

4. FORMA DE PAGAMENTO E RECURSOS FINANCEIROS

4.1. Conforme condições estabelecidas no Termo de Referência.

4.2. As despesas decorrentes desta contratação correrão à conta da dotação: 6.3.1.3.02.01.005 - Serviço de Tecnologia da Informação.

5. AUTORIZAÇÃO

5.1. Fica a empresa REDES VIX LTDA, inscrita no CNPJ 44.447.862/0001-32, representada pelo Sr. ERMELINDO FERNANDES CARNEIRO, AUTORIZADA a executar os serviços caracterizados nesta ORDEM DE SERVIÇO, ficando sujeita, no que couber, às normas e condições estabelecidas na Lei nº 14.133/21 e suas alterações e demais legislação pertinente.

5.2. O presente documento segue assinado pelo requisitante dos serviços e pelo Presidente do CRCES.



Documento assinado eletronicamente por **Walterleno Maifrede Noronha**, Presidente, em 14/01/2026, às 16:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wekson José Barbieri Mariano**, Analista - Sistemas / Desenvolvimento, em 14/01/2026, às 16:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1192527** e o código CRC **C3CF1E9E**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1192527

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

Processo nº 9079618110000798.000048/2025-57

1. IDENTIFICAÇÃO

Nº da OS:	01/2026
Data de Emissão:	14/01/2026
Área Requisitante:	TECNOLOGIA DA INFORMAÇÃO
Contratante:	CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
CNPJ:	28.163.343/0001-96
Endereço:	RUA AMÉLIA DA CUNHA ORNELAS, N.º 30, BENTO FERREIRA, VITÓRIA, ES, CEP: 29.050-620
Contratada:	REDES VIX LTDA
Empenho nº:	67/2026
Contrato nº:	49/2025

2. ESPECIFICAÇÃO DOS PRODUTOS

Subitem	Descrição	Valor Mensal	Valor Anual
1	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	R\$ 7.500,00	R\$ 90.000,00
2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	R\$ 3.000,00	R\$ 36.000,00
3	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	R\$ 3.166,67	R\$ 38.000,04
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	R\$ 8.000,00	R\$ 96.000,00
		R\$ 21.666,67	R\$ 260.000,04

3. INSTRUÇÕES COMPLEMENTARES

3.1. Todo detalhamento das especificações, prazos e demais informações encontram-se no Termo de Referência.

4. FORMA DE PAGAMENTO E RECURSOS FINANCEIROS

4.1. Conforme condições estabelecidas no Termo de Referência.

4.2. As despesas decorrentes desta contratação correrão à conta da dotação: 6.3.1.3.02.01.005 - Serviço de Tecnologia da Informação.

5. AUTORIZAÇÃO

5.1. Fica a empresa REDES VIX LTDA, inscrita no CNPJ 44.447.862/0001-32, representada pelo Sr. ERMELINDO FERNANDES CARNEIRO, AUTORIZADA a executar os serviços caracterizados nesta ORDEM DE SERVIÇO, ficando sujeita, no que couber, às normas e condições estabelecidas na Lei nº 14.133/21 e suas alterações e demais legislação pertinente.

5.2. O presente documento segue assinado pelo requisitante dos serviços e pelo Presidente do CRCES.



Documento assinado eletronicamente por **Walterleno Maifrede Noronha**, Presidente, em 14/01/2026, às 16:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wekson José Barbieri Mariano**, Analista - Sistemas / Desenvolvimento, em 14/01/2026, às 16:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1192527** e o código CRC **C3CF1E9E**.

Referência: Processo nº 9079618110000798.000048/2025-57

SEI nº 1192527

Documento assinado digitalmente
ERMELINDO FERNANDES CARNEIRO
Data: 14/01/2026 16:45:12-0300
Verifique em <https://validar.iti.gov.br>



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620
Telefone: (27) 3232-1600 - www.crc-es.org.br E-mail: diretoria@crc-es.org.br

PORTARIA CRCES Nº 003, DE 08 DE JANEIRO DE 2026.

Nomeia Fiscais Técnicos, Fiscais Substitutos, Gestores e Gestores Substitutos dos Acordos de Cooperação, Contratos, Convênios e Parcerias no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES.

O PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o disposto no art. 117 da Lei n.º 14.133, de 1º de abril de 2021, que determina o acompanhamento e a fiscalização da execução dos Contratos por representante da Administração, especialmente designado;

CONSIDERANDO o disposto nos arts. 39 e 50 e respectivos Anexos da Instrução Normativa n.º 5, de 25 de maio de 2017, da Secretaria de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão;

CONSIDERANDO que os Acordos de Cooperação e Convênios constituem-se em instrumentos afins, que também demandam fiscalização e gestão, conforme entendimento do Tribunal de Contas da União – TCU;

CONSIDERANDO a necessidade de redistribuição das atividades administrativas;

R E S O L V E:

Art. 1º. Nomear servidores para exercerem as funções de Fiscal Técnico, Fiscal Substituto, Gestor e Gestor Substituto, respondendo pela fiscalização, acompanhamento, avaliação das execuções e gestão dos Acordos de Cooperação, Contratos, Convênios e Parcerias, conforme listado no art. 3º deste instrumento.

Art. 2º. A equipe de gestores e fiscais de contrato deverá adotar o Decreto nº 11.246/2022, que dispõe sobre a atuação dos gestores e fiscais de contratos no âmbito da administração pública federal.

Art. 3º. Lista de Contratos ativos:

CONTRATO	PROCESSO SEI	EMPRESAS / INSTITUIÇÕES	FISCAL TÉCNICO	FISCAL SUBSTITUTO	GESTOR	GESTOR SUBSTITUTO
040/2025	9079618110000798.000074/2024-02	SAMP ESPÍRITO SANTO ASSISTÊNCIA MÉDICA SA	Vanessa Covre Rangel Marques	Elaine Leopoldino Ferreira	Kenia Cristina da Silva de March	Davis Berger Gobbi
048/2025	9079618110000798.000191/2024-68	TROGON COMÉRCIO DE INFORMÁTICA LTDA	Wekson José Barbieri Mariano	Elaine Leopoldino Ferreira	Kenia Cristina da Silva de March	Davis Berger Gobbi

049/2025	9079618110000798.000048/2025-57	REDES VIX LTDA	Wekson José Barbieri Mariano	Elaine Leopoldino Ferreira	Kenia Cristina da Silva de March	Davis Berger Gobbi
050/2025	9079618110000798.000056/2025-01	ARCO INFORMÁTICA LTDA	Wekson José Barbieri Mariano	Elaine Leopoldino Ferreira	Kenia Cristina da Silva de March	Davis Berger Gobbi

Art. 4º. Esta portaria entra em vigor na data de sua publicação e terá validade enquanto permanecer vigente o contrato.

Art. 5º. Dê-se ciência aos interessados e cumpra-se.

Contador **Walterleno Maifrede Noronha**
Presidente



Documento assinado eletronicamente por **Walterleno Maifrede Noronha, Presidente**, em 08/01/2026, às 17:02, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1184873** e o código CRC **6F4761C2**.

CRCES - Compras

De: CRCES - Compras
Enviado em: quarta-feira, 14 de janeiro de 2026 16:07
Para: 'ermelindo@redes.vix.br'
Assunto: Documentação para Assinatura e Informações de Pagamento – Redes Vix Ltda
Anexos: Nota Empenho nº 67.pdf; Ordem de Serviço nº 01-2026.pdf; Contrato nº 49-2025.pdf; Termo de Confidencialidade.pdf; Modelo de Declaracao do SIMPLES Nacional 2.docx

Boa tarde, prezados,

Segue em anexo a documentação referente à contratação: empenho, ordem de serviço, contrato e termo de confidencialidade.

Solicito, por gentileza, a assinatura do termo de confidencialidade e da ordem de serviço, com posterior devolutiva por e-mail.

Caso a empresa seja optante pelo **Simples Nacional**, solicitamos também o envio da **declaração**, conforme modelo em anexo.

Ressaltamos que as assinaturas poderão ser realizadas **digitalmente**, desde que contenham mecanismo que permita a verificação de sua autenticidade.

Por fim, pedimos que **Redes Vix Ltda** nos informe a **chave PIX** para efetivação do pagamento.

Agradecemos desde já!

Atenciosamente,

Maria Eduarda Storch

Administrativo - Compras

compras@crc-es.org.br / <https://crc-es.org.br>

Tel: + 55 (27) 3232-1634



Rua Amélia da Cunha Ornelas, N 30, Bairro Bento Ferreira - Vitória / ES - 29050-620

Economize papel. Imprima somente o que for indispensável. O Meio Ambiente agradece