
RESOLUÇÃO CRCES N.º 449, DE 15 DE DEZEMBRO DE 2022.

Institui a Política de Controle de Acesso Lógico no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES.

O **PLENÁRIO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO**, no uso de suas atribuições legais e regimentais, nos termos do inciso XVIII, art. 11, da Resolução n.º 342/2014;

CONSIDERANDO a necessária conformidade do CRCES aos termos da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018;

CONSIDERANDO a Portaria CRCES n.º 59, de 17 de maio de 2022, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Espírito Santo;

R E S O L V E:

CAPÍTULO I **DA INSTITUIÇÃO, APLICAÇÃO E CONTROLES DE ACESSO**

Art. 1º. Fica instituída a Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação, com vistas a possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas pelo Conselho Regional de Contabilidade do Espírito Santo - CRCES.

Art. 2º. Esta Política de Controle de Acesso Lógico aplica-se aos conselheiros, empregados, assessores, terceirizados, estagiários, aprendizes, colaboradores, usuários da rede visitante (sem fio) do CRCES, parceiros e/ou empresas contratadas pelo CRCES.

Art. 3º. A elaboração e atualização deste documento são de responsabilidade do Comitê de Segurança da Informação.

Art. 4º. O acesso a informações rotuladas como públicas e de uso interno não é restringido com controles de acesso que discriminam o usuário.

Art. 5º. O acesso a informações confidenciais e restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela Unidade Organizacional responsável.

Art. 6º. O acesso a alguns equipamentos de *hardware* e/ou *software* especiais (tais como equipamentos de diagnóstico de rede) é restrito aos profissionais da área de Informática (TI), com uso registrado, baseado nas necessidades do CRCES.

Art. 7º. Será dado a todos os usuários do CRCES, automaticamente, o acesso aos serviços básicos como correio eletrônico (*e-mail*), aplicações de produtividade e *browser* WEB.

§ 1º. Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente em cada Unidade Organizacional.

§ 2º. Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por solicitação feita ao proprietário da informação envolvida.

§ 3º. Quaisquer questões sobre controle de acessos privilegiados deverão ser direcionadas à Unidade Organizacional responsável pela informação.

CAPÍTULO II DOS TERMOS E DEFINIÇÕES

Art. 8º. Os seguintes termos são utilizados nesta Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação do CRCES com os significados específicos que se seguem:

I. Arquivo: agrupamento de registros que, geralmente, seguem uma regra estrutural e que possuem informações (dados);

II. Autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui;

III. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

IV. Credenciais de acesso: conjunto composto pelo nome de conta e respectiva senha, utilizado para o ingresso ou acesso (*login*) em equipamentos, rede ou sistema.;

V. Criptografia: arte e ciência de esconder o significado de uma informação de receptores não desejados;

VI. CSI-CRCES: Comitê de Segurança da Informação do CRCES;

VII. Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

VIII. Estações de trabalho: computador pessoal utilizado para trabalho nas Unidades Organizacionais;

IX. Gestor de Sistema: empregado oficialmente designado como gestor de determinado sistema de informação;

X. Integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades;

XI. Ponto de acesso sem fio: equipamento que compõe uma rede sem fio (*wireless*), concentrando as conexões de um ou mais equipamentos;

XII. Privilégio mínimo: conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades;

XIII. Programa: coleção de instruções que descrevem uma tarefa a ser realizada por um computador;

XIV. Recursos de armazenamento de dados corporativos: armazenamento de massa projetado para ambientes de grande escala e alta tecnologia;

XV. Recursos de TI: todo equipamento ou dispositivo que utiliza tecnologia da informação, bem como qualquer recurso ou informação que seja acessível por meio desses equipamentos ou dispositivos tecnológicos, tais como: impressoras, sistemas, programas, *softwares*, acessos à rede local, internet, VPN (rede particular virtual), *pendrives*, *smartcards*, *tokens*, *smartphones*, modems sem fio, *desktops*, pastas compartilhadas em rede, entre outros;

XVI. Rede local do CRCES: conjunto de recursos compartilhados por meio dos servidores de rede, *switches* e computadores clientes, por onde circulam as informações corporativas do CRCES;

XVII. Rede sem fio (*wireless*): sistema que interliga equipamentos utilizando o ar como via de transmissão por meio de ondas eletromagnéticas;

XVIII. Sistema de informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação;

XIX. Sistemas de mensageria: sistemas que permitem o envio e a recepção de mensagens de correio eletrônico ou de mensagens instantâneas entre usuários, dentro e fora da instituição;

XX. *Storages*: rede de área de armazenamento projetada para agrupar dispositivos de armazenamento de computador;

XXI. TI: Tecnologia da Informação;

XXII. TIC: Tecnologia da Informação e Comunicação: é um conjunto de recursos tecnológicos utilizados de forma integrada com um objetivo comum;

XXIII. Unidade Organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz;

XXIV. Usuário: pessoa física ou jurídica que opera algum sistema informatizado do CRCES;

XXV. *Web*: Rede Mundial de Computadores;

XXVI. Webconferência: reunião ou encontro virtual realizado pela Internet por meio de aplicativos ou serviço com possibilidade de compartilhamento de apresentações, voz, vídeos, textos e arquivos por meio da *web*.

CAPÍTULO III DO CADASTRAMENTO DE USUÁRIOS

Art. 9º. A criação de novas contas de acesso à rede se dará da seguinte forma:

I. para empregados e assessores: após a abertura de chamado no *helpdesk* ou serviço equivalente, informando o nome completo, a lotação e a matrícula do empregado;

II. para estagiários e menores aprendizes: após a abertura de chamado no *helpdesk* ou serviço equivalente, informando o nome completo, a lotação, matrícula do estagiário e a vigência do contrato; e

III. para prestadores de serviço: após a abertura de chamado pelo gestor do contrato no *helpdesk* ou serviço equivalente, informando o nome completo, Unidade Organizacional a que estiver vinculado, número e vigência do contrato, nome da empresa contratada e matrícula na empresa contratada (ou outro documento legalmente válido).

Parágrafo único. Nas eventuais substituições, caberá ao responsável informar o período para a configuração adequada da conta de acesso do empregado, assessor ou prestador de serviço.

Art. 10. As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato.

Art. 11. Caberá ao titular da Unidade Organizacional solicitar ao responsável pelo TI a liberação ou restrição de privilégios de acesso aos documentos de sua unidade.

Art. 12. Para evitar a expiração automática da conta de estagiários, menores aprendizes ou de prestadores de serviços, deverá ser aberto chamado pelo superior hierárquico imediato do estagiário ou do menor aprendiz, ou pelo gestor do contrato do prestador de serviços no *helpdesk* ou serviço equivalente, com antecedência mínima de 72 (setenta e duas) horas à expiração da conta.

Art. 13. Todos os usuários que utilizam aplicações e sistemas do CRCES devem assinar o Termo de Responsabilidade quanto ao uso dos recursos de trabalho fornecidos pelo colaborador ou terceirizado, conforme Anexo desta Resolução.

Art. 14. A assinatura do documento de que trata o artigo anterior indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos do CRCES relacionados ao ambiente de TI, incluindo as instruções contidas nesta Resolução, bem como as implicações legais decorrentes do não cumprimento do disposto no termo.

Art. 15. O gestor do contrato ficará responsável por recolher a assinatura dos prestadores de serviço no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCES, conforme Anexo desta Resolução e arquivá-lo junto à Diretoria Executiva.

Art. 16. O solicitante de acesso para empregados, assessores, estagiários ou menores aprendizes deverá recolher a assinatura destes no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCES, conforme Anexo desta Resolução e arquivá-lo junto à Diretoria Executiva.

Art. 17. Em casos excepcionais, poderão ser criadas contas para conselheiros, delegados, contadores membros de grupos e/ou comissões instituídas pela Presidência do CRCES ou empregados do Conselho Federal de Contabilidade ou de outros Conselhos Regionais de Contabilidade que estejam desempenhando serviços no CRCES, após abertura de chamado, via *helpdesk* ou serviço equivalente, pelo titular da Unidade Organizacional onde aquele atuará.

Parágrafo único. O Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCES, conforme o Anexo I, deverá ser assinado pelo conselheiro, delegado, membro de grupo e/ou comissão ou empregado do CFC e de outro CRC e ficará arquivado junto à Diretoria Executiva.

Art. 18. É de responsabilidade do gestor do contrato solicitar, via *helpdesk* ou serviço equivalente, o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.

Art. 19. O setor de recursos humanos deverá informar, por meio do *helpdesk* ou serviço equivalente, o desligamento e a movimentação de lotação de empregados, assessores, estagiários e de menores aprendizes para as providências de bloqueio e posterior eliminação da conta, se for o caso.

Art. 20. Não haverá identificação genérica e de uso compartilhado para acesso aos recursos de rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer do TI, acerca da possibilidade de aceitação dos riscos associados.

Art. 21. As novas contas de acesso à rede serão compostas por nome e sobrenome, sendo a forma padrão o nome e o último sobrenome, separados por ponto.

Parágrafo único. Caso a forma padrão incorra em homonímia com conta já existente, será escolhida forma alternativa do seguinte modo:

- a) nome e o penúltimo sobrenome completo, separados por ponto; e
- b) letras iniciais do prenome e o último sobrenome completo, separados por ponto.

Art. 22. No ato da criação de conta de acesso à rede, será automaticamente criada conta dos serviços de correio eletrônico (*e-mail*), mensageria e agenda correspondente, bem como de outros serviços que utilizem a mesma base de dados para autenticação.

Art. 23. Após a criação da conta solicitada, a equipe do TI deverá informar ao solicitante a criação da conta e a senha de acesso inicial, juntamente com as instruções para a sua alteração.

Art. 24. Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.

Parágrafo único. No caso de descumprimento do disposto neste item, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis, tanto o titular das credenciais quanto aquele que as utilizar indevidamente.

CAPÍTULO IV DA POLÍTICA DE SENHAS

Art. 25. A identificação de usuários que operam a rede local do CRCES deve ser feita mediante a autenticação usuário-senha.

Art. 26. A senha cadastrada é pessoal, intransferível e confidencial.

Art. 27. A senha deverá observar as seguintes regras de formação:

I. não pode conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos;

II. deve conter, no mínimo, 12 (doze) caracteres; e

III. deve conter caracteres de três das quatro categorias seguintes:

a) caracteres alfabéticos maiúsculos;

b) caracteres alfabéticos minúsculos;

c) caracteres numéricos; e

d) caracteres especiais, não alfabéticos (por exemplo: !, \$, #, %).

Art. 28. A senha cadastrada terá prazo de validade de 90 (noventa) dias, ao fim do qual o usuário deverá cadastrar nova senha.

Parágrafo único. A nova senha não poderá ser igual às últimas 4 (quatro) senhas anteriormente utilizadas no período de 12 (doze) meses.

Art. 29. Após 5 (cinco) tentativas erradas, o usuário ficará bloqueado, necessitando recadastrar nova senha.

Art. 30. Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Art. 31. Em caso de comprometimento comprovado de segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

Art. 32. Independentemente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

CAPÍTULO V DOS ACESSOS

Seção I DO ACESSO À REDE

Art. 33. Apenas poderão ser conectadas à rede cabeada do CRCES microcomputadores e notebooks previamente autorizados pela TI.

§ 1º. Exceções devem ser comunicadas à Diretoria Executiva do CRCES, justificando a necessidade e o prazo de utilização.

§ 2º. As exceções autorizadas deverão, obrigatoriamente, adotar os padrões definidos pela Política de Segurança da Informação do CRCES, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, uma vez que o CRCES não fornecerá licenças para o funcionamento de microcomputadores particulares.

Art. 34. Microcomputadores e dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

Parágrafo único. O usuário, antes de acessar a rede visitante, deverá se identificar e concordar com o termo de uso da rede sem fio.

Art. 35. O TI poderá desconectar das redes, cabeada e sem fio, qualquer dispositivo que constitua ameaça à segurança da informação.

Art. 36. Computadores com acesso à rede deverão ser desligados ou bloqueados na ausência do usuário.

Seção II **DO ACESSO À INTRANET E À INTERNET**

Art. 37. Os acessos a portais da Internet e aos demais serviços disponíveis na Intranet do CRCES serão efetuados, preferencialmente, por meio da rede local e deverão ser identificados por usuário.

§ 1º. Os rastros de acesso deverão, no mínimo, identificar usuários, endereço IP, URL acessada, data e hora.

§ 2º. O TI deverá reter os rastros de acesso pelo prazo mínimo fixado pela política de log.

Art. 38. É proibido o acesso a sítios que tratem de pornografia, pedofilia, erotismo e correlatos; de racismo; de ferramentas para invasão e evasão de sistemas; de compartilhamento de arquivos; e de apologia e incitação a crimes.

Parágrafo único. O TI poderá utilizar *software* específico que realizará o bloqueio automático desses sítios.

Art. 39. Os acessos a *sites* e serviços disponíveis na Internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança da rede do CRCES, cuja operacionalização é de responsabilidade do TI.

Art. 40. Os setores do CRCES devem definir, com base nas categorias de conteúdo fornecidas pelo TI, os perfis de filtro de conteúdo a serem aplicados a cada uma de suas unidades.

§ 1º. As solicitações de criação ou alteração nas permissões de acesso deverão ser formalizadas e juntadas em processo próprio.

§ 2º. Os titulares das Unidades Organizacionais do CRCES devem fiscalizar o bom uso dos acessos à Internet e solicitar ajustes e restrições, em caso de má utilização.

§ 3º. Mediante solicitação do responsável pelo setor, o TI poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

Art. 41. O TI poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos como vídeo conferências e acesso a visitantes.

Art. 42. Todas as operações de acesso realizadas serão registradas para fins de auditoria.

Art. 43. Não será admitido burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis.

Seção III

DO ACESSO REMOTO A SISTEMAS DE INFORMAÇÃO

Art. 44. O acesso remoto à rede corporativa do CRCES deve ser realizado somente para atender aos interesses de trabalho.

Art. 45. Compete ao TI definir os perfis de acesso, aplicando técnicas de autenticação e de segurança.

§ 1º. O acesso remoto, no âmbito da rede corporativa, deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

§ 2º. O acesso remoto à rede corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

§ 3º. A permissão para realização de acesso remoto à rede corporativa deve ser solicitada à área de administração da rede pela Coordenação ou área superior à qual o usuário da rede está subordinado, com definição do prazo de validade e horários para se realizar o acesso; e

§ 4º. O acesso remoto à rede corporativa será gravado, para posterior auditoria, em logs contendo data e hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada.

Art. 46. Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas do CRCES devem se submeter ao mecanismo de controle de acesso, levando-se em consideração os privilégios necessários ao acesso a cada tipo de informação.

Art. 47. Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação ao TI.

Art. 48. Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, o Comitê de Segurança da Informação deverá ser imediatamente acionado para tomar as providências necessárias e sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do CRCES.

Art. 49. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação.

CAPÍTULO VI DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 50. O correio eletrônico é o recurso corporativo para comunicação a ser utilizado de modo compatível com o exercício da função, sem comprometer a imagem do CRCES nem o tráfego de dados na rede de computadores da instituição.

§ 1º. Todas as mensagens eletrônicas enviadas e recebidas nos domínios do CRCES terão registrados os dados: data e hora do envio ou recebimento, remetente e destinatário.

§ 2º. O TI deverá implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

§ 3º. O TI poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por Unidade Organizacional e por usuário.

§ 4º. O TI não acessará mensagens individuais de caixas de *e-mail*, salvo para atender aos seguintes objetivos:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

II. recuperar conteúdo de interesse do CRCES, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

IV. atender à determinação judicial; e

V. realizar a recuperação de mensagens do *backup*, a pedido do próprio usuário.

§ 5º. O envio de mensagens a componentes da lista de endereços e grupos de *e-mails* do CRCES restringir-se-á a assuntos de interesse geral da instituição.

§ 6º. A exclusão de caixas postais ocorrerá com o desligamento do usuário.

Art. 51. São vedadas as seguintes ações relacionadas à utilização do correio eletrônico:

I. acesso ou tentativa de acesso à caixa postal em desacordo com o previsto no § 4º do Art. 50;

II. envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições do usuário, incluindo as que contém ofensas, comentários discriminatórios e pornografia; e

III. adulteração de dados referentes à origem da mensagem nos campos de controle e cabeçalho.

Parágrafo único. Para os fins deste artigo, considera-se armazenado o *e-mail* aberto e mantido na caixa postal do usuário.

Art. 52. O TI prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

CAPÍTULO VII DA UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 53. O sistema de arquivos compreende um conjunto de pastas armazenadas em servidor de arquivos e compartilhadas em rede, que podem ser compartilhadas entre todos os usuários ou restrito a usuários de determinado setor ou de determinado projeto.

Art. 54. O TI realizará o *backup* dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de *Backup*.

Parágrafo único. O *backup* de arquivos de pastas de usuário armazenadas nas estações de trabalho é de responsabilidade do usuário.

Art. 55. O TI poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas dos setores.

Art. 56. O TI não acessará os arquivos armazenados nas pastas dos setores e dos usuários, salvo nas seguintes situações:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

II. recuperar conteúdo de interesse do CRCES, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Presidência do CRCES ou da Diretoria Executiva;

IV. atender à solicitação judicial; e

V. realizar a recuperação de arquivos do backup, a pedido do usuário.

Art. 57. Os casos omissos serão dirimidos pela Comissão de Segurança da Informação do CRCES.

Art. 58. Esta resolução entra em vigor na data de sua assinatura.

Contadora **Carla Cristina Tasso**
Presidente

Aprovada na 1650ª Reunião Plenária, realizada em 15 de dezembro de 2022

ANEXO

TERMO DE RESPONSABILIDADE

Pelo presente termo, declaro ter conhecimento da Política de Controle de Acesso Lógico do Conselho Regional de Contabilidade do Espírito Santo - CRCES, disponível para consulta no portal do CRCES.

Declaro que estou recebendo uma conta de rede e/ou e-mail corporativo e/ou acesso a aplicações e sistemas com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas de acordo com a Política de Controle de Acesso Lógico do CRCES e de que qualquer alteração feita sob minha identificação, oriunda de minha autenticação e autorização, é de minha responsabilidade.

Estou ciente, ainda, de minha responsabilidade pelo dano que posso causar pelo descumprimento da Política de Controle de Acesso Lógico do CRCES ao realizar uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Vitória/ES, ____ de _____ de 20 ____.

Nome
Matrícula
Unidade Organizacional

Nome
Unidade Organizacional
(titular da Unidade Organizacional ou gestor do contrato, para o caso de terceirizados)