RESOLUÇÃO CRCMG N.º 442, DE 17 DE DEZEMBRO DE 2021.

Dispõe sobre a Política de Controle de Acesso Lógico do CRCMG.

O **CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS,** no uso de suas atribuições legais e regimentais,

Considerando o Decreto n.º 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, em especial o inciso II do artigo 15;

Considerando o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

Considerando as normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações;

Considerando a Portaria CRCMG n.º 63, de 24 de abril de 2019, que criou o Comitê de Segurança da Informação (CSI) do CRCMG;

R E S O L V E:

CAPÍTULO I
Definição e competências

Art. 1º Fica estabelecida a Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação, para possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas pelo Conselho Regional de Contabilidade de Minas Gerais (CRCMG).

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 CRCMG, parceiros e empresas e/ou empresas contratadas pelo CRCMG.

Art. 3º Para o acesso a informações rotuladas como públicas, não são utilizados controles que discriminam o usuário.

Art. 4º O acesso às informações confidenciais e restritas será permitido apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso for

registrado e aprovado pela Matriz de Permissões de Acesso da Unidade Organizacional responsável.

Art. 5º O acesso a alguns equipamentos de *hardware* e/ou *software* especiais (tais como equipamentos de diagnóstico de rede) é restrito aos profissionais com uso registrado, baseado nas necessidades do CRCMG.

Art. 6º O acesso a serviços básicos, como correio eletrônico (e-mail), aplicações de produtividade e *browser* WEB, será concedido a todos os usuários do CRCMG mediante solicitação da Unidade Organizacional ou da Gerência Administrativa e Financeira (GEADF), responsável pela gestão de Recursos Humanos.

Parágrafo único. Essas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente em cada Unidade Organizacional.

CAPÍTULO II
TERMOS E DEFINIÇÕES

Art. 7º Os seguintes termos são utilizados nesta Política de Controle de Acesso Lógico com relação aos ativos e aos sistemas de informação do CRCMG, com os significados específicos que se seguem:

I - Controle de acesso lógico: controle de acesso a locais ou sistemas por meio de *login* e senha, certificado digital ou biometria;

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

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

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

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

VI - Criptografia: arte e ciência de esconder o significado de uma informação de receptores não desejados;

VII - CSI-CRCMG: Comitê de Segurança da Informação do CRCMG;

VIII - Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

IX - Estações de trabalho: computador pessoal utilizado para trabalho nas Unidades Organizacionais;

X - Gestor de Sistema: empregado oficialmente designado como gestor de determinado sistema de informação;

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

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

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

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

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

XVI - 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*, *modens* sem fio, *desktops*, pastas compartilhadas em rede, entre outros;

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

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

XIX - 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;

XX - 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;

XXI - *Storage*: rede de área de armazenamento projetada para agrupar dispositivos de armazenamento de computador;

XXII - TI: Tecnologia da Informação*;*

XXIII - TIC: Tecnologia da Informação e Comunicação. Trata-se de um conjunto de recursos tecnológicos utilizados de forma integrada com um objetivo comum*;*

XXIV - Unidade Organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz*;*

XXV - Usuário: pessoa física ou jurídica que opera algum sistema informatizado do CRCMG;

XXVI - Web: Rede Mundial de Computadores;

XXVII - 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
CADASTRAMENTO DE USUÁRIOS

Art. 8º A criação de novas contas de acesso à rede se dará da seguinte forma:

I - para empregados e assessores da presidência: após a abertura de chamado, no Help Desk, pela Unidade Organizacional na qual o funcionário será lotado, informando o nome completo e a matrícula e os sistemas e recursos aos quais ele terá acesso;

II - para estagiários e menores aprendizes: após a abertura de chamado, no Help Desk, pela GEADF (RH), informando o nome completo, a Unidade Organizacional de lotação, matrícula do estagiário e a vigência do contrato;

III - para prestadores de serviço: após a abertura de chamado, no Help Desk, pelo gestor do contrato, informando o nome completo, a Unidade Organizacional de lotação, o número e a vigência do contrato, o nome e a matrícula (ou outro documento legalmente válido) da empresa contratada.

§ 1º Nas eventuais substituições, caberá ao responsável informar à Gerência da Tecnologia da Informação (Getin) o período para a configuração adequada da conta de acesso do empregado ou prestador de serviço.

§ 2º A GEADF deverá informar, por meio do Help Desk, 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. 9º As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato.

§ 1º Rescindido o contrato antes do fim de sua vigência, deverá ser aberto, no Help Desk, um chamado pelo superior hierárquico imediato do estagiário ou do menor aprendiz ou pelo gestor do contrato do prestador de serviços, com antecedência mínima de cinco dias úteis antes da expiração da conta.

§ 2º Para evitar a expiração automática da conta, em caso de renovação de contrato de estagiários, menores aprendizes ou de prestadores de serviços, deverá ser aberto, no Help Desk, um chamado pelo superior hierárquico imediato do estagiário ou do menor aprendiz ou pelo gestor do contrato do prestador de serviços, com antecedência mínima de 5 (cinco) dias úteis antes da expiração da conta.

§ 3º É de responsabilidade do gestor do contrato solicitar, via Help Desk, o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.

Art. 10. Caberá ao titular da Unidade Organizacional solicitar à Getin, via Help Desk, a liberação ou restrição de privilégios de acesso aos documentos de sua Unidade.

Art. 11. Todos os usuários que utilizam aplicações e sistemas do CRCMG devem assinar o Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCMG, conforme o Anexo I desta resolução.

§ 1º A assinatura do documento de que trata o *caput* deste artigo indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos do CRCMG relacionados ao ambiente de TI (incluindo as instruções contidas nesta resolução), bem como com as implicações legais decorrentes do não cumprimento do disposto no termo.

§ 2º A GEADF deverá recolher a assinatura do empregado, assessor, estagiário, menor aprendiz ou prestador de serviço no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCMG, conforme o Anexo I desta resolução, e arquivá-la.

Art. 12. Em casos excepcionais, exceto nos sistemas desenvolvidos para este público, poderão ser criadas contas para conselheiros, membro de Grupo de Estudos Técnicos ou comissão que estejam desempenhando suas atribuições no CRCMG, após abertura de chamado via Help Desk pelo titular da Unidade Organizacional na qual este atuará.

Parágrafo único. O Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCMG, conforme o Anexo I desta resolução, deverá ser assinado pelo conselheiro, membro de Grupo de Estudos Técnicos ou comissão a que se refere o *caput* deste artigo e ficará arquivado na Diretoria Executiva.

Art. 13. 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 da Getin, acerca da possibilidade de aceitação dos riscos associados.

Art. 14. As novas contas de acesso à rede e/ou e-mail 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:

I - nome e o penúltimo sobrenome completo, separados por ponto;

II - letras iniciais do prenome e o último sobrenome completo, separados por ponto.

Art. 15. Na abertura da solicitação via Help Desk, deverá ser indicada a necessidade de criação de conta dos serviços de correio eletrônico (e-mail) e da intranet, bem como de outros serviços que utilizem a mesma base de dados para autenticação.

Art. 16. As informações sobre a conta e a senha de acesso inicial, juntamente com as instruções para a sua alteração, serão enviadas pela Getin por meio de chamado a ser aberto no Help Desk.

Art. 17. Em nenhuma hipótese, será admitido o empréstimo ou o compartilhamento de credenciais de acesso.

Parágrafo único. No descumprimento dos casos tratados neste artigo, 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
POLÍTICA DE SENHAS

Art. 18. A identificação de usuários que operam a rede local e utilizam as aplicações do CRCMG deve ser feita mediante a autenticação com usuário e senha.

Art. 19. A senha cadastrada é pessoal, intransferível e confidencial.

Art. 20. A senha deverá observar as seguintes regras de formação:

I - não pode conter “CRCMG” ou nome e sobrenome do usuário;

II - deve conter, no mínimo, dez caracteres;

III - deve conter os quatro caracteres das quatro categorias seguintes, com, no mínimo, um caractere:

a) alfabético maiúsculo;

b) alfabético minúsculo;

c) numérico;

d) especial, não alfabético (por exemplo: !, $, #, @, %, etc).

Art. 21. Após cinco tentativas erradas, o usuário ficará bloqueado, necessitando recadastrar nova senha.

Parágrafo único. Para aplicativos web desenvolvidos pelo CRCMG, o usuário ficará bloqueado por um período de tempo pré-determinado, após exceder o limite de tentativas de *login*.

Art. 22. Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Art. 23. 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. 24. Independentemente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas, expostas ou acessíveis ao acesso de terceiros, sendo o proprietário da senha o responsável legal por qualquer prática indevida cometida.

CAPÍTULO V
ACESSO À REDE

Art. 25 Apenas microcomputadores e *notebooks* previamente fornecidos pela Getin poderão ser conectados à rede cabeada do CRCMG.

§ 1º Exceções devem ser comunicadas à Getin do CRCMG via HelpDesk, pelo responsável pela unidade demandante, 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 CRCMG, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados.

Art. 26. Microcomputadores e dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

§ 1º Somente terão permissão ao serviço os conselheiros efetivos e suplentes do CRCMG, dispositivos corporativos do CRCMG, líderes do CRCMG e quem estes designarem através de solicitação feita no Help Desk.

§ 2º O usuário, antes de acessar a rede visitante, deverá concordar com o termo de uso da rede sem fio para ter acesso ao serviço.

Art. 27. A Getin poderá desconectar das redes cabeadas e sem fio qualquer dispositivo que constitua ameaça à segurança da informação ou prejuízo à imagem do CRCMG e/ou aos recursos tecnológicos do CRCMG.

Art. 28. Computadores com acesso à rede deverão ser desligados ou bloqueados na ausência do usuário, ainda que momentânea.

CAPÍTULO VI
ACESSO À INTRANET E À INTERNET

Art. 29. Os acessos a portais da internet e aos demais serviços disponíveis na intranet do CRCMG 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 A Getin deverá manter registros (*logs*) de acesso aos recursos de TI do CRCMG.

Art. 30. 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; de apologia e incitação a crimes.

Parágrafo único. A Getin poderá utilizar *software* específico que realizará o bloqueio automático desses sítios.

Art. 31. 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 CRCMG, cuja operacionalização é de responsabilidade da Getin.

Art. 32. Com base nas categorias de conteúdo padronizadas pelo CRCMG, os perfis de filtro de conteúdo são aplicados para todos os funcionários, que devem acessar somente conteúdo para fins de realização do seu trabalho.

§ 1º As solicitações de criação ou alteração nas permissões de acesso deverão ser formalizadas por meio de chamados abertos no Help Desk.

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

§ 3º Mediante solicitação do titular da Unidade Organizacional, a Getin poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

Art. 33. A Getin poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos, como videoconferências e acesso a visitantes.

Art. 34. Todas as operações de acesso realizadas serão registradas para fins de auditoria.

Art. 35. 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.

CAPÍTULO VII
ACESSO REMOTO A SISTEMAS DE INFORMAÇÃO

Art. 36. O acesso remoto à rede corporativa do CRCMG deve ser realizado somente para atender aos interesses de trabalho.

Art. 37. Compete à Getin definir os perfis de acesso, aplicando técnicas de autenticação e de segurança, entre elas:

I - o acesso remoto, no âmbito da rede corporativa, deve ser provido por meio de canal criptografado, preferencialmente configurado pela Getin;

II - o acesso remoto é permito aos líderes do CRCMG;

III - o acesso remoto à rede corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

IV - a permissão para se realizar acesso remoto à rede corporativa deve ser solicitada à Getin, via Help Desk, pelo líder imediato a que o Usuário da Rede está subordinado, com definição do prazo de validade e horários para se realizar o acesso;

V - 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. 38. Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas do CRCMG devem se submeter ao mecanismo de controle de acesso, levando-se em consideração os privilégios necessários ao acesso a cada tipo de informação.

Art. 39. Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Getin.

Art. 40. Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a Getin deverá ser imediatamente acionada para tomar as providências necessárias para 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 CRCMG.

Art. 41. São vedadas as seguintes ações relacionadas ao acesso remoto:

I - acesso ou tentativa de acesso a equipamentos da rede do CRCMG para equipamentos fora das dependências do CRCMG, através de quaisquer recursos de acesso remoto, exceto o uso da Gerência de Tecnologia da Informação, para finalidade específica de trabalho relacionado ao CRCMG, desde que aprovado pelo responsável pela Gerência de Tecnologia da Informação;

II - o envio ou armazenamento de informações de propriedade do CRCMG para equipamento particular. Se o fizer para fins de suas atividades do CRCMG, deverá ser excluído permanentemente de seu equipamento, após a finalização dos trabalhos;

III - em casos de uso de equipamentos particulares, deixar de utilizar senha de acesso no perfil que utiliza para acesso remoto ao CRCMG.

CAPÍTULO VIII
UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 42. 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 CRCMG nem o tráfego de dados na rede de computadores da instituição.

§ 1º Todas as mensagens eletrônicas enviadas e recebidas nos domínios do CRCMG terão os seguintes dados registrados: data e hora do envio ou recebimento, remetente e destinatário, inclusive o conteúdo dos e-mails excluídos, que fica registrado e armazenado por 30 (trinta) dias.

§ 2º A Getin deverá implantar mecanismos que previnam, na medida do possível, o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

§ 3º A Getin poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por usuário.

§ 4º O e-mail corporativo é para uso estritamente corporativo e, sendo assim, é de domínio do CRCMG. As contas de e-mails corporativos de propriedade do CRCMG são de acesso irrestrito do Conselho, podendo ser abertos pelo CRCMG ou por outros usuários, a critério do superior hierárquico, para atender às seguintes finalidades:

I - verificar a obtenção, retenção, uso e divulgação de informações por meios ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

II - recuperar conteúdo de interesse do CRCMG, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

III - atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

IV - atender à determinação judicial;

V - atender à demanda de serviços da Unidade Organizacional.

§ 5º Cabe à Gerência Administrativa e Financeira adotar medidas de segurança para evitar que e-mails com dados pessoais e/ou sensíveis do funcionário sejam entregues no e-mail corporativo.

§ 6º O envio de mensagens aos grupos de e-mails do CRCMG através do serviço de e-mail corporativo será restrito a assuntos de interesse geral da instituição ou do Sistema CFC/CRCs. A permissão de envio para cada grupo estará restrita aos usuários definidos pela Diretoria Executiva do CRCMG.

§ 7º A exclusão de caixas postais ocorrerá com o desligamento do usuário, após prévia autorização do superior hierárquico, através de Help Desk.

Art. 43. 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 artigo 42;

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

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

IV - para cadastro em lojas, entidades financeiras, escolas, recebimento de *mailings*, entre outros assuntos não compatíveis com as atividades do CRCMG.

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

Art. 44. A Getin prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

CAPÍTULO IX
UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 45. 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 restritas a usuários de determinada Unidade Organizacional ou de determinado projeto.

Art. 46. A Getin 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. 47. A Getin poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas das Unidades Organizacionais.

Art. 48. A Getin não acessará os arquivos armazenados nas pastas das Unidades Organizacionais e dos usuários, salvo o gerente e o assistente de Tecnologia da Informação, nas seguintes situações:

I - verificar a obtenção, retenção, uso e divulgação de informações por meios ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

II - recuperar conteúdo de interesse do CRCMG, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

III - atender a demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Presidente do CRCMG ou do Diretor Executivo;

IV - atender à solicitação judicial;

V - realizar a recuperação de arquivos do *backup*, a pedido do usuário;

VI - análise da disponibilização de conteúdo em pastas para orientar sobre o melhor uso dos recursos de armazenamento;

VII - tratamento de demandas pontuais, quando solicitado via Help Desk e dentro da própria Unidade Organizacional.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Art. 49. A elaboração e atualização deste documento é de responsabilidade do Comitê de Segurança da Informação.

Art. 50. Os casos omissos serão dirimidos pelo Comitê de Segurança da Informação do CRCMG.

Art. 51. Esta resolução entra em vigor na data de sua publicação.

Contadora Rosa Maria Abreu Barros
Presidente

Aprovada na 12ª Reunião Plenária, realizada em 17 de dezembro de 2021.
Publicada no Diário Oficial da União, seção 1, n.º 6, em 10 de janeiro de 2022, na página 202.

ANEXO I

Termo de Responsabilidade

Pelo presente termo, declaro ter conhecimento da Política de Controle de Acesso Lógico do Conselho Regional de Contabilidade de Minas Gerais (CRCMG), disponível para consulta no portal do CRCMG.

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 CRCMG 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 CRCMG 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.

Belo Horizonte, ____ de _____ de 20__.

Nome
Matrícula
Unidade Organizacional

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