RESOLUÇÃO CRCMG N.º 439, DE 17 DE DEZEMBRO DE 2021.

Institui a Política de Incidentes de Segurança da Informação do CRCMG.

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

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término;

R E S O L V E:

CAPÍTULO I
POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade de Minas Gerais (CRCMG).

Art. 2º A Política de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação do CRCMG e visa orientar o funcionamento do processo de gestão de incidentes de segurança digital e não digital da informação, de forma que sejam tratados adequadamente, reduzindo ao máximo os impactos para a entidade.

Art. 3º Para os efeitos desta resolução, entende-se por:

I - Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

II - Atividade crítica: atividade que deve ser executada de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permita atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - Atividade maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema, serviço ou rede;

IV - Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

V - Colaborador: pessoa física ou jurídica envolvida em qualquer atividade do CRCMG, seja de natureza permanente, temporária ou excepcional, sendo delegado seccional, membro de Grupo de Estudos Técnicos, estagiário ou prestador de serviços;

VI - Evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas, ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

VII - Fluxo de Trabalho de Incidentes: predefinição de etapas que devem ser tomadas para lidar com um tipo particular de incidente;

VIII - Gerenciamento de incidentes: processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um sistema, serviço ou rede seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado;

IX - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

X - Omissão: a não observância das políticas de segurança definidas pelo CRCMG.

CAPÍTULO II
OBJETIVO

Art. 4º A Política de Incidentes de Segurança da Informação do CRCMG tem por objetivos:

I - diminuir os danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência;

II - promover a efetiva e eficaz Política da Segurança da Informação no CRCMG;

III - diminuir o número total de incidentes de segurança da informação envolvendo o CRCMG, por meio de prevenção sistemática dos eventos e eliminação de situações que permitam a ocorrência desses incidentes.

CAPÍTULO III
ABRANGÊNCIA

Art. 5º A Política de Incidentes de Segurança da Informação abrange todos os incidentes, confirmados ou sob suspeita, que envolvam o nome ou a propriedade do Conselho Regional de Contabilidade de Minas Gerais, bem como qualquer conselheiro, funcionário, estagiário, menor aprendiz ou colaborador, no exercício da sua função ou relação com o CRCMG.

Art. 6º A lista a seguir exemplifica, mas não esgota, os possíveis incidentes de segurança da informação tratados nesta política:

I - violar a Política de Controle de Ativos de Tecnologia da Informação do CRCMG;

II - violar uma política de segurança, explícita ou implícita;

III - realizar acesso indevido ou não autorizado a instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCMG que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

IV - realizar acesso indevido ou não autorizado a dados, informações e documentos mantidos, tratados e controlados pelo CRCMG que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

V - conectar dispositivo de tecnologia à rede do CRCMG que esteja contaminado com vírus de computador detectado por mecanismo automatizado ou pessoal qualificado;

VI - violar norma de utilização ou configuração de dispositivo de tecnologia da informação, conectado ou não à rede do CRCMG, detectada automática ou manualmente;

VII - vazar dados pessoais;

VIII - utilizar credenciais de autenticação (senhas) por indivíduo não proprietário delas ou de outrem;

IX - facilitar fluxo de comunicação de rede caracterizado como atividade maliciosa por detecção de padrão ou análise manual, ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades maliciosas;

X - omitir a comunicação de fragilidade de segurança conhecida em processo, instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCMG;

XI - violar direito autoral ou propriedade intelectual de qualquer natureza;

XII - realizar tentativa de fraude, bem ou malsucedida, independentemente do dano causado;

XIII - quaisquer outros eventos que constituam violação de requisito de segurança estabelecido pela Política de Segurança da Informação do CRCMG, tenham eles origem no próprio CRCMG ou em grupos externos.

CAPÍTULO IV
COMPETÊNCIAS E RESPONSABILIDADES

Seção I
COMPETÊNCIAS

Art. 7º Ao Comitê Gestor de Privacidade e Proteção de Dados compete:

I - conduzir o processo de Gestão de Incidentes de Segurança da Informação, quando se tratar de incidentes de segurança com dados pessoais, juntamente com o Comitê de Segurança da Informação e com o encarregado de dados pessoas, em conformidade com a Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG;

II - investigar incidentes de segurança com dados pessoais, com o levantamento da cadeia de custódia e segurança das evidências;

III - acompanhar os planos de tratamento junto aos responsáveis pelos incidentes de segurança com dados pessoais e a criação de indicadores e relatórios;

IV - realizar as análises dos pós-incidentes (*post mortem*) para identificação e tratamento de causas raízes e aprimoramento de processos do CRCMG e do próprio processo de gestão de incidentes de segurança com dados pessoais.

Art. 8º Ao Comitê de Segurança da Informação compete:

I - conduzir o processo de Gestão de Incidentes de Segurança da Informação e, quando se tratar de incidentes de segurança com dados pessoais, atuar juntamente com o Comitê Gestor de Privacidade e Proteção de Dados e com o encarregado de dados pessoas, em conformidade com a Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG;

II - executar os procedimentos de tratamento de incidentes de segurança das informações não digitais definidos nesta política no surgimento de qualquer denúncia e/ou detecção automatizada e registrar os incidentes tratados;

III - investigar incidentes de segurança da informação, com o levantamento da cadeia de custódia e segurança das evidências;

IV - comunicar aos líderes responsáveis incidentes de segurança da informação que envolvam recursos ou informações sob sua responsabilidade;

V - acompanhar os planos de tratamento junto aos responsáveis pelos incidentes e a criação de indicadores e relatórios;

VI - realizar as análises dos pós-incidentes (*post mortem*) para identificação e tratamento de causas raízes e aprimoramento de processos do CRCMG e do próprio processo de gestão de incidentes de segurança da informação;

VII - definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCMG;

VIII - avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

IX - dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

Art. 9º À Gerência de Tecnologia da Informação compete:

I – comunicar ao Comitê de Segurança da Informação e, quando aplicável, ao Comitê Gestor de Privacidade e Proteção de Dados, qualquer evento de segurança ou fragilidade sobre o qual tenha sido notificada, que possa causar prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CRCMG;

II – comunicar ao Comitê de Segurança da Informação e, quando aplicável, ao Comitê Gestor de Privacidade e Proteção de Dados, todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que tenha identificado ou sobre as quais tenha sido notificada, que possam indicar a possibilidade de incidentes;

III - executar os procedimentos de tratamento de incidentes de segurança da informação das informações digitais definidos nesta política, no surgimento de qualquer denúncia e/ou detecção automatizada, e registrar os incidentes tratados, conforme o modelo e operacionalização e a serem definidos em procedimento específico;

IV - definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCMG;

V - avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

VI - dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área;

VII - elaborar, anualmente, relatório estatístico do número de incidentes para fins de acompanhamento pelo CRCMG;

VIII - manter comunicação efetiva com o Comitê de Segurança da Informação, o Comitê Gestor de Privacidade e Proteção de Dados e o encarregado de dados pessoais sobre possíveis ameaças e ações que deverão ser adotadas para mitigação dos riscos relacionados a incidentes de segurança da informação.

Seção II
RESPONSABILIDADES

Art. 10. Os líderes, ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes pré-definidos pelo Comitê Gestor de Privacidade e Proteção de Dados e pelo Comitê de Segurança da Informação, com a devida urgência.

Art. 11. São responsabilidades de todos os conselheiros, funcionários, estagiários, menores aprendizes e colaboradores:

I - estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado;

II - notificar à Gerência de Tecnologia da Informação qualquer evento de segurança ou fragilidade observada que possa causar prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CRCMG;

III - informar imediatamente à Gerência de Tecnologia da Informação todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

§ 1º Na apuração dos incidentes de segurança da informação, será considerada a boa ou má-fé que possa estar envolvida na realização do incidente de segurança, ou seja, o elemento subjetivo que venha a favorecer a vulnerabilidade dos dados pessoais.

§ 2º Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos conselheiros, funcionários, estagiários, menores aprendizes e colaboradores, sob o risco de violar a política de segurança digital e não digital e da informação, bem como provocar danos aos sistemas, serviços ou recursos tecnológicos digitais ou não digitais.

CAPÍTULO V
VIOLAÇÕES E SANÇÕES

Art. 12. Os conselheiros, empregados, estagiários, menores aprendizes e colaboradores que presenciarem o descumprimento de alguma das regras acima têm o dever de denunciar tal infração.

Art. 13. O descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

CAPÍTULO VI
REVISÃO E ATUALIZAÇÃO

Art. 14. A Política de Incidentes de Segurança da Informação deverá ser revista e atualizada sempre que necessário.

Art. 15. Esta resolução entra em vigor na data de sua publicação.

Contadora Rosa Maria Abreu Barros
Presidente

Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.
Publicada no Diário Oficial da União, seção 1, n.º 3, em 05 de janeiro de 2022, na página 59.