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.

Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

RESOLUÇÃO CRCMG Nº 440, DE 17 DE DEZEMBRO DE 2021

Institui a Política de Notificação de Incidentes de Segurança com Dados Pessoais 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 obrigam-se a garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término; resolve:

CAPÍTULO I

POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Minas Gerais (CRCMG).

Art. 2º Para os efeitos desta resolução, entende-se por:

I - Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso significa que um dado é considerado pessoal quando permite a identificação direta ou indireta da pessoa natural;

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IV - Tratamento: toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transparência, difusão ou extração;

V - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso desta política, o CRCMG;

VI - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - Comitê Gestor de Privacidade e Proteção de Dados (CGPPD): comitê responsável pela avaliação dos mecanismos de tratamento, privacidade e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento com vistas ao cumprimento das disposições da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do CRCMG;

IX - Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional;

X - Notificação: ato ou efeito de informar ou de dar a conhecer sobre uma ocorrência e/ou incidente de segurança com dados pessoais.

CAPÍTULO II

OBJETIVO

Art. 3º A Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG tem por objetivo descrever os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

Art. 4º Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

CAPÍTULO III

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 5º A identificação do incidente pode ocorrer das seguintes formas:

I - denúncia por parte de titular ou terceiro;

II - reporte por parte ou operador;

III - pelo emprego de ferramentas automatizadas que detectam vazamentos de dados;

IV - através de comunicação feita por conselheiros, funcionários, estagiários, menores aprendizes e colaboradores do CRCMG, conforme disposto na Política de Incidentes de Segurança da Informação.

Art. 6º Todas as violações de dados pessoais devem ser comunicadas ao encarregado pelo tratamento de dados pessoais do CRCMG, sem demora injustificada, para registro e avaliação das medidas a serem tomadas.

Art. 7º Em caso de um incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao encarregado pelo tratamento de dados pessoais do CRCMG, pelo sistema disponível no portal do CRCMG, no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente.

Art. 8º No caso do titular ou terceiro, a comunicação de um incidente de segurança com dados pessoais poderá ser enviada ao encarregado pelo tratamento de dados pessoais do CRCMG, pelo sistema disponível no portal do CRCMG, preferencialmente, em até 48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.

Art. 9º Na comunicação, o operador, terceiro ou titular dos dados pessoais deverá descrever sucintamente o incidente ocorrido, atentando para informações tais como:

I - descrever a natureza da violação dos dados pessoais, incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registros de dados pessoais em causa;

II - descrever as consequências prováveis da violação de dados pessoais;

III - descrever as medidas adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Art. 10. O encarregado pelo tratamento de dados pessoais do CRCMG será responsável pelo registro e análise inicial do incidente e pela resposta sobre o incidente relatado.

Art. 11. Após o registro e a análise inicial do incidente, o encarregado pelo tratamento de dados pessoais do CRCMG compartilhará a comunicação com o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) e com o Comitê de Segurança da Informação (CSI) do CRCMG, para que seja realizada a avaliação das medidas a serem tomadas.

§ 1º Caso necessário, o CGPPD ou o CSI poderá acionar a Gerência de Tecnologia da Informação (Getin) e a Assessoria Jurídica (Asjur) do CRCMG.

§ 2º O CGPPD e o CSI não realizam procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

Art. 12. As partes envolvidas devem seguir as orientações do encarregado pelo tratamento de dados pessoais do CRCMG, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais.

Art. 13. As partes envolvidas devem manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto incidente com dados pessoais e a identificação do autor do incidente.

CAPÍTULO IV

NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 14. O CRCMG notificará a ANPD e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

§ 1º O CRCMG deverá avaliar internamente a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular.

§ 2º Para a avaliação interna, deverão ser analisados os incidentes que envolvam especialmente:

I - dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou que tenham o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade;

II - volume de dados envolvidos, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

§ 3º A notificação não será necessária se o responsável pelo tratamento puder demonstrar, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

Art. 15. Caso necessária, a notificação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 16. Caso não seja possível fornecer todas as informações no momento da notificação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que, no momento da notificação preliminar, deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

Art. 17. A notificação à ANPD será feita por intermédio do encarregado pelo tratamento de dados pessoais do CRCMG.

Parágrafo único. O encarregado pelo tratamento de dados pessoais do CRCMG comunicará o incidente com dados pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pelo CGPPD, pelo CSI, pela Getin e pela Asjur do CRCMG.

Art. 18. O encarregado pelo tratamento de dados pessoais do CRCMG ainda tem como responsabilidade:

I - aprovar e autorizar a divulgação de comunicado aos titulares envolvidos no incidente com dados pessoais;

II - validar quaisquer comunicados ao público, imprensa e usuários referentes ao incidente com dados pessoais;

III - orientar e/ou informar as equipes interessadas a respeito das práticas a serem adotadas com relação ao incidente com dados pessoais;

IV - coordenar todas as ações decorrentes do incidente com dados, com o intuito de mitigar os impactos percebidos;

V - atuar como porta-voz do CRCMG perante a ANPD, demais autoridades competentes e os usuários, supervisionando os contatos e comunicações com o público, decorrentes do incidente com dados pessoais, dentre outras atividades.

Art. 19. Esta resolução entra em vigor na data da sua publicação.

Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

DECISÃO Nº 28, DE 2 DE SETEMBRO DE 2021

O Plenário do Conselho Regional de Enfermagem de São Paulo - Coren-SP, neste ato, legal e regimentalmente representado pelo Presidente e pela Primeira Secretária desta Autarquia,

CONSIDERANDO a necessidade de adequar o normativo do Conselho Regional de Enfermagem de São Paulo - Coren-SP, que regulamenta a concessão de diárias e passagens, ao disposto na Resolução Cofen nº 0471/2015, alterada pelas Resolução Cofen nº 590/2018 e Resolução Cofen nº 607/2019;

CONSIDERANDO os princípios basilares que regem a Administração Pública, conforme estabelecido no artigo 37, caput, da Constituição Federal, bem como os princípios da razoabilidade do interesse público e da economicidade dos atos de gestão;