CÂMARA MUNICIPAL DE
MONTES CLAROS

Plano de Resposta à Incidentes de Segurança

Lei 13.709 de 24 de agosto de 2018

Lei Complementar nº 103 de 28 de março de 2023 – Câmara Municipal de Montes Claros/MG

Sumário

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, as organizações brasileiras passaram a ter a obrigação legal de proteger os dados pessoais que coletam e processam.

A Autoridade Nacional de Proteção de Dados (ANPD) também emite diretrizes para garantir a conformidade com a lei. Incidentes de segurança que envolvem o vazamento ou perda de dados pessoais podem ter consequências graves, tanto para os indivíduos afetados quanto para as organizações responsáveis.

Assim, a elaboração de um plano de resposta a incidentes de segurança é essencial para mitigar os danos e garantir o cumprimento das obrigações legais.

Introdução

Este plano visa estabelecer diretrizes claras e procedimentos a serem seguidos em caso de incidentes de segurança que comprometam a integridade, confidencialidade, ou disponibilidade de dados pessoais no âmbito interno da Câmara Municipal de Montes Claros/MG.

A resposta rápida e eficaz é fundamental para minimizar os impactos, proteger os direitos dos titulares de dados e garantir a conformidade com a LGPD e as normativas da ANPD.

Conceitos Principais

Incidente de Segurança: Qualquer evento que resulte em comprometimento da segurança de dados pessoais, incluindo, mas não se limitando a, vazamentos, acessos não autorizados, perda, destruição ou alteração de dados pessoais.

Dados Pessoais: Qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Referências à LGPD

Artigo 46: Estabelece que os agentes de tratamento de dados devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais.

> Art. 46. 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.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Artigo 48: Determina que o controlador deve comunicar à ANPD e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação 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; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Artigo 50: Prevê a implementação de programas de governança em privacidade, que incluam um plano de resposta a incidentes.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Prevenção de Incidentes de Segurança

A prevenção é a primeira linha de defesa contra incidentes de segurança. Vejamos as principais medidas preventivas:

Criptografia: Adotar criptografia para proteger dados pessoais armazenados e transmitidos.

Controles de Acesso: Implementar controles rigorosos de acesso, garantindo que apenas pessoas autorizadas tenham acesso a dados pessoais.

Monitoramento Contínuo: Monitorar continuamente os sistemas de TI para detectar e responder a atividades suspeitas ou anômalas.

Capacitação e Conscientização: Realizar treinamentos regulares com funcionários sobre a importância da segurança da informação e da proteção de dados pessoais.

Auditorias Regulares: Conduzir auditorias periódicas para garantir a conformidade com as políticas de segurança e identificar possíveis vulnerabilidades.

Gerenciamento para o Registro em Caso de Incidentes de Segurança

Procedimentos em caso de Incidentes de Segurança:

Em caso de incidente de segurança, as etapas abaixo devem ser seguidas:

1 - Identificação e Contenção:

- ✓ Detectar o incidente de segurança e identificar sua natureza e extensão.
- ✓ Conter o incidente para evitar que se espalhe ou cause mais danos.

2 - Avaliação de Impacto:

- ✓ Avaliar o impacto do incidente sobre os dados pessoais envolvidos, determinando o nível de risco para os titulares dos dados.
- ✓ Identificar os dados comprometidos e o possível prejuízo causado aos titulares.

3 - Notificação:

- ✓ Notificar a ANPD sobre o incidente, conforme exigido pelo Artigo 48 da LGPD.
- ✓ Informar os titulares dos dados afetados, explicando as medidas tomadas para mitigar os danos.

4 - Remediação:

- ✓ Implementar medidas corretivas para evitar a recorrência do incidente.
- ✓ Revisar e atualizar as políticas de segurança, se necessário.

5 - Relatório e Documentação:

- ✓ Documentar todas as ações tomadas durante a resposta ao incidente.
- ✓ Elaborar um relatório detalhado para análise posterior e para auditorias futuras.

Recomendações Finais

Planejamento Contínuo: Revisar e atualizar regularmente o plano de resposta a incidentes de segurança, levando em consideração novas ameaças e mudanças no ambiente regulatório.

Teste do Plano: Realizar simulações periódicas para testar a eficácia do plano e treinar a equipe envolvida na resposta a incidentes, inclusive na parte de sistemas operados pelo setor de Tecnologia da Informação.

Cultura de Segurança: Promover uma cultura organizacional que valorize a segurança da informação e a proteção de dados pessoais em todas as atividades da Câmara Municipal de Montes Claros/MG.

Plano elaborado pela Comissão Permanente de Proteção de Dados, instituída pela Lei Complementar nº 103 de 28 de março de 2023 no âmbito da Câmara Municipal de Montes Claros/MG.

Versão 30/08/2024.

CÂMARA MUNICIPAL DE
MONTES CLAROS

Rua Urbino Viana, nº 600, Vila Guilhermina,
Montes Claros/MG, CEP: 39400-087

Telefone: (38) 3690-5516