



CÂMARA MUNICIPAL DE
MONTES CLAROS

Plano de Resposta a 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

Resolução CD/ANPD nº 15 de 24 de abril de 2024

Sumário

1 – Introdução	2
2 – Objetivos	3
3 – Conceitos Principais	4
4 – Incidentes de Segurança com Dados Pessoais	5
5 – Comunicação e Registro em Caso de Incidentes de Segurança	6
6 – Prevenção de Incidentes de Segurança	8
7 – Recomendações Finais	9
8 – Anexo I – Formulário de Comunicação Interna de Incidente de Segurança	10



Introdução

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. Este plano será revisado e atualizado regularmente, levando em consideração novas ameaças e mudanças no ambiente regulatório.



Objetivos

O plano de resposta a incidentes de segurança 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.

Assegurar uma resposta rápida e eficaz é fundamental para minimizar os impactos, proteger os direitos dos titulares de dados e garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e as normativas da Autoridade Nacional de Proteção de Dados (ANPD).



Conceitos Principais

Dado Pessoal: Qualquer informação relacionada a uma pessoa natural identificada ou identificável.

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.

Tratamento de Dados Pessoais: Toda 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, transferência, difusão ou extração.

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.

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.

Incidentes de Segurança com Dados Pessoais

Conforme estabelecido no artigo 46 da LGPD, os agentes de tratamento de dados devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais. Ainda nos termos da referida lei, o 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. Além disso, o artigo 50 da LGPD prevê que controladores e operadores poderão formular regras de boas práticas e de governança para o tratamento de dados pessoais, podendo ser implementado programa de governança em privacidade que inclua um plano de resposta a incidentes.

De acordo com o artigo 5º do Regulamento de Comunicação de Incidente de Segurança da ANPD, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024, define que o incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

- I - dados pessoais sensíveis;
- II - dados de crianças, de adolescentes ou de idosos;
- III - dados financeiros;
- IV - dados de autenticação em sistemas;
- V - dados protegidos por sigilo legal, judicial ou profissional;

ou

- VI - dados em larga escala.

Comunicação e Registro em Caso de Incidentes de Segurança

Qualquer fato que possa configurar incidente de segurança com dados pessoais deverá ser imediatamente comunicado a comissão permanente de tratamento e proteção de dados da Câmara. Essa comunicação poderá ser feita através do Formulário de Comunicação Interna de Incidente de Segurança (anexo I) ou pelo e-mail lgpd@montesclaros.mg.leg.br.

Caso o incidente seja confirmado, as etapas abaixo devem ser seguidas:

1 - Identificação e Contenção:

- ✓ Identificar a natureza, categoria e extensão do incidente de segurança.
- ✓ Adotar medidas para conter o incidente evitando 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.

Comunicação e Registro em Caso de Incidentes de Segurança

3 - Notificação:

- ✓ Notificar a ANPD sobre o incidente, no prazo de três dias úteis, conforme artigo 6º do Regulamento de Comunicação de Incidente de Segurança da ANPD (Resolução CD/ANPD nº 15/2024).
- ✓ Comunicar aos titulares dos dados afetados, no prazo de três dias úteis, conforme artigo 9º do Regulamento de Comunicação de Incidente de Segurança da ANPD (Resolução CD/ANPD nº 15/2024).

4 - Remediação:

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

5 - Relatório e Registro:

- ✓ Elaborar um relatório detalhado para análise posterior e para auditorias futuras.
- ✓ Manter o registro dos incidentes de segurança, inclusive daqueles não comunicados à ANPD, pelo prazo mínimo de cinco anos.

Prevenção de Incidentes de Segurança

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

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: Orientar funcionários sobre a importância da segurança da informação e da proteção de dados pessoais.

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



Recomendações Finais

Boas Práticas no Tratamento de Dados Pessoais: O tratamento de dados pessoais deve ser realizado de forma cautelosa, obedecendo as diretrizes estabelecidas na Lei Geral de Proteção de Dados.

Senhas de Acesso: As senhas de acesso a sistemas e e-mails institucionais são pessoais, sigilosas e intransferíveis e só podem ser utilizadas pelo usuário cadastrado.

Mensagens Suspeitas: Sempre verifique a procedência de e-mails e desconfie de links ou arquivos anexados à mensagem. Em caso de dúvidas, entrar em contato com o 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.



Anexo I

FORMULÁRIO DE COMUNICAÇÃO INTERNA DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

1 - IDENTIFICAÇÃO DO COMUNICANTE

Nome: _____
Cargo/Setor: _____
Telefone/Ramal: _____
E-mail institucional: _____

2 - DADOS DO INCIDENTE

Data de conhecimento: ____/____/_____
Local/Setor onde ocorreu: _____
Sistema(s) ou serviço(s) afetado(s): _____

3 - DESCRIÇÃO DO INCIDENTE

4 - CATEGORIA E NATUREZA DOS DADOS ENVOLVIDOS

Dados pessoais
 Dados pessoais sensíveis
 Dados de crianças, adolescentes ou idosos
 Dados financeiros
 Dados de autenticação em sistemas (login, senha)
 Dados protegidos por sigilo (legal, judicial ou profissional)
 Dados em larga escala

5 - ESTIMATIVA DE IMPACTO

Número estimado de titulares afetados: _____
Grupos específicos envolvidos (se houver): _____

6 - MEDIDAS EMERGENCIAIS ADOTADAS ATÉ O MOMENTO

Comunicação à chefia imediata
 Comunicação ao setor de TI
 Alteração de senhas/acessos
 Outra (especificar): _____

7 - OBSERVAÇÕES ADICIONAIS OU SUSPEITA DE AUTORIA

Data do preenchimento: ____/____/_____

Assinatura do comunicante: _____

Recebido por (EPD ou Comissão de Proteção de Dados):

Nome: _____
Data: ____/____/_____
Assinatura: _____



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

Atualizado em 30/06/2025.

Comissão Permanente de Tratamento e Proteção de Dados:

Carla Bianca Durazzo Costa
Encarregada de Proteção de Dados

Renato Marcelo Pereira Souza
Membro de Apoio da Comissão

Wallisson Mendes Santos
Assessor de Tratamento de Dados



CÂMARA MUNICIPAL DE **MONTES CLAROS**

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