Procedimento de Notificação de Incidentes de Segurança da Informação

Data da última atualização: fevereiro/2026.

1. Objetivo

Este documento tem como objetivo estabelecer as diretrizes e procedimentos para a identificação, tratamento, registro e notificação de incidentes de segurança da informação, no âmbito da BRASILMED AUDITORIA MÉDICA E SERVIÇOS LTDA, que possam acarretar risco ou dano relevante aos titulares de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) e a Resolução CD/ANPD Nº 15, de 27 de maio de 2024.

Visa garantir a pronta comunicação ao Controlador, à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, quando aplicável, minimizando impactos e assegurando a transparência e a responsabilização da Brasilmed como Operadora de dados.

2. Definições

Para os fins deste capítulo, aplicam-se as seguintes definições:

- **ANPD (Autoridade Nacional de Proteção de Dados):** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.
- **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No contexto da Brasilmed, o Controlador são seus clientes que contratam os serviços especializados.
- **Dados Pessoais:** Informação relacionada a pessoa natural identificada ou identificável.
- **Dados Pessoais Sensíveis:** 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. No contexto da Brasilmed, dados de saúde são frequentemente tratados.
- **Incidente de Segurança da Informação:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação da segurança de dados pessoais, como acesso não autorizado, destruição, perda, alteração, difusão ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

- **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador. A Brasilmed atua como Operadora.
- **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Vazamento de Dados:** Incidente de segurança que resulta na divulgação não autorizada de dados pessoais.

3. Critérios para Identificação de Incidentes que Requerem Notificação

Um incidente de segurança da informação será considerado passível de notificação ao Controlador, à ANPD e/ou aos titulares quando houver risco ou dano relevante aos titulares. A avaliação de risco e dano levará em conta, mas não se limitará a:

- **Natureza dos dados afetados:** Atingimento de dados pessoais sensíveis (especialmente dados de saúde), dados financeiros ou dados de identificação que possam levar a fraudes.
- **Gravidade do incidente:** Potencial de causar discriminação, violação da integridade física, moral ou da reputação, fraudes financeiras, uso indevido de identidade, ou qualquer outra forma de dano material ou imaterial.
- **Número de titulares afetados:** Grande volume de dados ou titulares envolvidos.
- **Abrangência do incidente:** Duração, extensão e impacto do incidente nas operações e na privacidade dos titulares.
- **Medidas de segurança existentes:** Existência e eficácia de medidas técnicas e organizacionais de segurança que poderiam ter evitado ou mitigado o incidente.
- **Irreversibilidade ou dificuldade de reversão do dano:** Quando as consequências do incidente são difíceis de serem revertidas ou mitigadas.

4. Procedimentos de Notificação

A Brasilmed, na sua condição de Operadora, seguirá os seguintes procedimentos:

4.1. Notificação Interna e ao Controlador

1. **Detecção e Avaliação:** Ao tomar ciência de qualquer incidente de segurança da informação, confirmado ou sob suspeita, o colaborador responsável ou a equipe de TI deve

imediatamente reportar o ocorrido ao Encarregado de Dados (DPO) da Brasilmed e ao Fornecedor de Serviços da Segurança da Informação.

2. **Análise Preliminar:** O DPO e o Fornecedor de Serviços da Segurança da Informação realizarão uma análise preliminar para determinar a natureza, extensão e impacto potencial do incidente, bem como se envolve dados pessoais e se há risco ou dano relevante aos titulares.

3. **Comunicação ao Controlador:** Caso o incidente envolva dados pessoais tratados em nome de um Controlador, a Brasilmed notificará o Controlador imediatamente após a ciência do incidente, fornecendo todas as informações disponíveis para que o Controlador possa cumprir suas obrigações legais. Esta comunicação será realizada por meio dos canais de comunicação previamente acordados com o Controlador.

4. **Suporte ao Controlador:** A Brasilmed prestará todo o suporte necessário ao Controlador para a investigação do incidente, mitigação dos danos e preparação das notificações à ANPD e aos titulares, conforme a legislação vigente.

4.2. Notificação à ANPD e aos Titulares (Responsabilidade do Controlador)

5. **Responsabilidade Primária:** A responsabilidade pela notificação à ANPD e aos titulares dos dados é do Controlador.

6. **Apoio da Brasilmed:** A Brasilmed, como Operadora, fornecerá ao Controlador todas as informações e evidências necessárias para que este possa realizar as notificações à ANPD e aos titulares de forma completa e tempestiva, incluindo: Descrição detalhada do incidente.

7. Dados pessoais afetados.

8. Medidas técnicas e de segurança utilizadas para a proteção dos dados.

9. Riscos e danos relevantes aos titulares.

10. Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.

11. Informações de contato do Encarregado de Dados da Brasilmed para esclarecimentos.

5. Prazos de Comunicação

- **Notificação da Brasilmed ao Controlador:** A comunicação do incidente de segurança da informação da Brasilmed (Operadora) ao Controlador deve ocorrer imediatamente

após a ciência do incidente, de modo a permitir que o Controlador cumpra seus prazos legais.

- **Notificação do Controlador à ANPD:** O Controlador deve comunicar a ANPD sobre o incidente de segurança em um prazo de até 3 (três) dias úteis, contado da data do conhecimento do incidente, conforme estabelecido pela Resolução CD/ANPD Nº 15/2024.
- **Notificação do Controlador aos Titulares:** A comunicação aos titulares deve ser realizada em prazo razoável, conforme determinação da ANPD ou avaliação do Controlador, considerando a gravidade e o risco do incidente.

6. Conteúdo Obrigatório das Notificações

As notificações a serem realizadas pelo Controlador à ANPD e, quando aplicável, aos titulares, com base nas informações fornecidas pela Brasilmed, deverão conter, no mínimo:

- **Descrição do incidente de segurança:** Detalhes sobre o que aconteceu, incluindo a data e hora da ocorrência e da detecção, se possível.
- **Tipo de dados pessoais afetados:** Categorias e quantidade aproximada de dados pessoais envolvidos (e.g., nome, CPF, dados de saúde, endereço).
- **Titulares de dados pessoais afetados:** Número aproximado de titulares afetados.
- **Medidas técnicas e de segurança:** Descrição das medidas de segurança e privacidade que estavam em vigor para a proteção dos dados, incluindo as medidas de segurança implementadas para conter o incidente.
- **Riscos e danos relevantes:** Avaliação dos riscos e danos relevantes aos titulares decorrentes do incidente.
- **Medidas para mitigar os efeitos:** Descrição das medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo aos titulares.
- **Informações de contato:** Canais de contato do Encarregado de Dados do Controlador e, se pertinente, da Brasilmed, para que os titulares possam obter mais informações.

7. Responsabilidades das Equipes Envolvidas

- **Todos os Colaboradores da Brasilmed:** Têm o dever de reportar imediatamente qualquer suspeita ou confirmação de incidente de segurança da informação ao seu superior direto e ao DPO da Brasilmed.

- **Equipe de Tecnologia da Informação (TI):** Responsável pela detecção, contenção e remediação técnica dos incidentes, além de fornecer informações técnicas detalhadas ao DPO.
- **Encarregado de Dados (DPO) da Brasilmed:** Lidera a resposta a incidentes, coordena a comunicação interna e com o Controlador, avalia o risco e dano, e garante a conformidade com a LGPD e regulamentações da ANPD.
- **Fornecedor de Serviços da Segurança da Informação:** Apoia o DPO na avaliação de incidentes, na tomada de decisões estratégicas e na implementação de planos de ação.
- **Diretoria da Brasilmed:** Garante os recursos necessários para a gestão de incidentes e a conformidade com a política.
- **Controlador:** Responsável final pela notificação à ANPD e aos titulares, com base nas informações e suporte fornecidos pela Brasilmed.

8. Registro e Documentação dos Incidentes

A Brasilmed manterá um registro detalhado de todos os incidentes de segurança da informação, independentemente de terem sido notificados externamente. Este registro incluirá, no mínimo:

- Data e hora da descoberta do incidente.
- Descrição detalhada do incidente.
- Dados pessoais e sistemas afetados.
- Medidas de contenção e remediação adotadas.
- Avaliação de risco e dano aos titulares.
- Decisão sobre a necessidade de notificação ao Controlador, ANPD e/ou titulares.
- Datas e detalhes das comunicações realizadas (internas e externas).

9. Vigência e Revisão da Política

Este procedimento entra em vigor na data de sua publicação. Será revisado anualmente ou sempre que houver alterações significativas na legislação, nas regulamentações da ANPD, nas operações da Brasilmed ou na avaliação de riscos, para garantir sua contínua adequação e eficácia.

BRASILMED AUDITORIA MÉDICA E SERVIÇOS LTDA.