**Política de Gestão de Incidentes de Segurança de Dados Pessoais**

**1. Objetivo**

Estabelecer diretrizes e procedimentos para a identificação, comunicação, contenção, tratamento e notificação de incidentes de segurança envolvendo dados pessoais, com o objetivo de minimizar impactos aos titulares dos dados e garantir conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

**2. Abrangência**

Esta política se aplica a todos os colaboradores, prestadores de serviço, unidades organizacionais, sistemas e processos que realizem operações de tratamento de dados pessoais no âmbito da [Nome da Instituição/Órgão].

**3. Definições**

Dado pessoal: Informação relacionada à pessoa natural identificada ou identificável.

Dado pessoal sensível: Dado sobre origem racial ou étnica, convicção religiosa, opinião política, etc.

Incidente de segurança: Qualquer evento adverso confirmado ou sob suspeita relacionado à violação de dados pessoais, como acessos não autorizados, vazamentos, perda, alteração ou destruição acidental ou ilícita.

Encarregado: Pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

Controlador: Pessoa natural ou jurídica que decide sobre o tratamento dos dados pessoais.

**4. Princípios Orientadores**

Transparência: Os titulares devem ser informados, de forma clara, sobre incidentes que possam afetá-los.

Responsabilidade: A instituição deve agir de forma diligente e tempestiva na resposta a incidentes.

Segurança da informação: Aplicação de medidas técnicas e administrativas adequadas para proteção dos dados.

**5. Diretrizes Gerais**

**5.1. Identificação e Comunicação Interna**

Todo colaborador que identificar ou suspeitar de um incidente de segurança deve comunicar imediatamente à área responsável (ex: Segurança da Informação, Encarregado de Dados ou Comitê de Privacidade).

Um canal oficial deverá estar disponível para esse tipo de comunicação.

**5.2. Avaliação Inicial**

A área técnica avaliará a natureza, extensão e impacto do incidente.

Será verificado se há risco ou dano relevante aos titulares dos dados pessoais.

**5.3. Resposta e Contenção**

Ações emergenciais devem ser adotadas para conter o incidente e impedir sua propagação.

As evidências do incidente devem ser preservadas para análise posterior.

**5.4. Notificação**

Quando houver risco ou dano relevante, o incidente será notificado à Autoridade Nacional de Proteção de Dados (ANPD) e, se necessário, aos titulares, conforme o Art. 48 da LGPD.

A notificação deverá conter, no mínimo:

* Descrição da natureza dos dados afetados;
* Informações sobre os titulares envolvidos;
* Medidas técnicas e de segurança utilizadas;
* Motivos da demora (se não for imediata);
* Ações adotadas para mitigar os danos.

**5.5. Registro**

Todos os incidentes devem ser registrados em relatório próprio contendo data, causa, impacto, ações tomadas e lições aprendidas.

**5.6. Plano de Resposta e Melhoria Contínua**

A instituição deverá manter um plano de resposta a incidentes, com revisão periódica.

Serão promovidas ações de capacitação, simulações e revisões para melhoria contínua dos processos de segurança.

**6. Papéis e Responsabilidades**

|  |  |
| --- | --- |
| Função | Responsabilidades |
| Encarregado (DPO) | Articular resposta e comunicação com a ANPD e titulares; manter registros atualizados |
| Equipe de TI / SI | Investigar causas, corrigir falhas técnicas, manter medidas preventivas |
| Comitê de Privacidade | Avaliar impacto, riscos e estratégias de mitigação |
| Colaboradores | Comunicar qualquer anomalia ou suspeita de incidente |

**7. Sanções e Penalidades**

O descumprimento desta política poderá acarretar a responsabilização funcional ou contratual do colaborador, conforme legislação aplicável e normativos internos.

**8. Vigência e Atualizações**

Esta política entra em vigor na data de sua aprovação e será revisada anualmente ou sempre que houver mudança relevante nos processos, legislação ou estrutura organizacional.