PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA EM DADOS

Empresa: TechSolutions Ltda.
Área Responsável: Departamento de Segurança da Informação e Privacidade (DSIP)
Data de Criação: 10/10/2023
Última Revisão: 10/10/2023

---

1. OBJETIVO

Este plano tem como objetivo estabelecer diretrizes e procedimentos para identificar, conter, investigar, corrigir e reportar incidentes de segurança envolvendo dados pessoais, garantindo a conformidade com a LGPD e minimizando impactos aos titulares dos dados e à organização.

---

2. DEFINIÇÕES

- **Incidente de Segurança:** Qualquer evento adverso, confirmado ou sob suspeita, que possa comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais.
- **Dados Pessoais:** Qualquer informação relacionada a uma pessoa identificada ou identificável.
- **Violação de Dados:** Incidente que resulta na destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais.

---

3. EQUIPE DE RESPOSTA A INCIDENTES

- **Coordenador:** João Silva (Diretor de Segurança da Informação)
- **Membros:**
    - Maria Oliveira (Especialista em Privacidade)
    - Carlos Souza (Analista de Segurança)
    - Ana Costa (Jurídico)

- Pedro Lima (Relações Públicas)

---

4. ETAPAS DO PLANO DE RESPOSTA A INCIDENTES

4.1. Identificação do Incidente

- **Ações:**
  - Monitoramento contínuo de sistemas e logs.
  - Notificação de colaboradores sobre possíveis incidentes.
  - Uso de ferramentas de detecção de anomalias.
- **Exemplo:** Um colaborador reporta o envio acidental de um e-mail contendo dados pessoais de clientes para um destinatário não autorizado.

4.2. Contenção do Incidente

- **Ações:**
  - Isolar sistemas afetados.
  - Revogar acessos não autorizados.
  - Solicitar a exclusão de e-mails enviados indevidamente.
- **Exemplo:** Bloquear o acesso ao e-mail do destinatário não autorizado e solicitar a devolução ou exclusão dos dados.

4.3. Investigação e Análise

- **Ações:**
  - Coletar evidências (logs, registros de acesso, etc.).
  - Determinar a causa raiz do incidente.
  - Avaliar o impacto nos titulares dos dados e na organização.
- **Exemplo:** Verificar quantos clientes foram afetados e quais dados foram expostos.

4.4. Notificação e Comunicação

- **Ações:**
  - Notificar a Autoridade Nacional de Proteção de Dados (ANPD) em até 72 horas, se necessário.
  - Comunicar os titulares dos dados afetados, quando houver risco significativo.
  - Preparar comunicados à imprensa, se necessário.

- **Exemplo:** Enviar um e-mail aos clientes afetados explicando o ocorrido e as medidas tomadas.

4.5. Correção e Recuperação

- **Ações:**
    - Implementar correções técnicas (ex.: atualizações de software, revisão de políticas).
    - Realizar treinamentos para evitar recorrências.
    - Restaurar sistemas e dados afetados.
- **Exemplo:** Reforçar a política de envio de e-mails com dados sensíveis e realizar treinamento para colaboradores.

4.6. Revisão e Melhoria

- **Ações:**
    - Realizar uma análise pós-incidente.
    - Documentar lições aprendidas.
    - Atualizar o plano de resposta a incidentes.
- **Exemplo:** Incluir verificações adicionais no processo de envio de e-mails.

---

5. COMUNICAÇÃO INTERNA E EXTERNA

- **Interna:**
    - Informar a alta administração e os colaboradores envolvidos.
- **Externa:**
    - Notificar a ANPD e os titulares dos dados, conforme exigido pela LGPD.
    - Emitir comunicados à imprensa, se necessário.

---

6. TREINAMENTO E CONSCIENTIZAÇÃO

- Realizar treinamentos periódicos para colaboradores sobre proteção de dados e procedimentos de resposta a incidentes.
- Simular cenários de incidentes para testar a eficácia do plano.

---

7. DOCUMENTAÇÃO E REGISTROS

- Manter registros detalhados de todos os incidentes, incluindo:
    - Descrição do incidente.
    - Medidas tomadas.
    - Impactos identificados.
    - Lições aprendidas.

---

8. REFERÊNCIAS

- Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.
- Normas ISO/IEC 27001 e 27002.

Este é um exemplo básico e pode ser adaptado conforme o tamanho e a complexidade da organização. Se precisar de mais detalhes ou ajustes, é só avisar!