



Plano de Resposta a Incidentes de Vazamento de Dados Pessoais

VendeAI Tecnologia

POL-VDA-04 — versão 1.0

1 Introdução

Este Plano de Resposta a Incidentes de Vazamento de Dados Pessoais tem por objetivo estabelecer o processo que a VendeAI Tecnologia (“VendeAI”) deve seguir para detectar, conter, investigar e comunicar incidentes de segurança envolvendo dados pessoais, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), e as boas práticas da norma ISO/IEC 27005.

2 Definições

Incidente de vazamento de dados — qualquer evento de divulgação não autorizada, perda, acesso indevido, modificação, destruição ou comprometimento de dados pessoais tratados pela VendeAI, seus sistemas ou fornecedores.

Equipe de Gestão de Incidentes — grupo responsável por coordenar a resposta a um incidente, liderado pelo DPO e composto, conforme a natureza do incidente, pelo CTO, pela liderança comercial e por consultoria jurídica externa quando necessário. Na estrutura atual da VendeAI, a Equipe de Gestão de Incidentes é formada por Gustavo Schewinski (CTO/DPO) e Nicolas Ignacio Ryberg (CEO), podendo ser ampliada conforme o crescimento da empresa.

3 Resposta a incidentes

3.1 Detecção e notificação

Qualquer colaborador, prestador de serviço ou parceiro que identifique ou suspeite de um incidente de vazamento de dados deve reportar **imediatamente** ao DPO, por e-mail (contato@vendeaitecnologia.com.br) ou pelo canal interno de incidentes definido pela empresa.

3.2 Classificação

O incidente é classificado pela Equipe de Gestão de Incidentes em uma matriz de gravidade:

Gravidade	Critério
Alta	Vazamento de dados sensíveis ou de grande volume de titulares; risco relevante a direitos e liberdades dos titulares
Média	Vazamento de dados pessoais comuns, volume limitado, risco moderado
Baixa	Incidente contido sem exposição efetiva de dados a terceiros não autorizados

3.3 Resposta e recuperação

A Equipe de Gestão de Incidentes elabora e executa plano de contenção, investigação e documentação do incidente, com o objetivo de interromper a causa, restaurar a segurança dos sistemas afetados e preservar evidências para a investigação.

3.4 Investigação e análise

Após a contenção, é conduzida investigação de causa raiz, com registro detalhado (forense, quando aplicável) dos sistemas, dados e usuários afetados, para subsidiar a comunicação e a adoção de

medidas corretivas.

3.5 Comunicação e notificação

O DPO coordena a comunicação interna (liderança da VendeAI) e externa do incidente, incluindo, quando exigido pela LGPD ou por obrigação contratual:

- notificação à Autoridade Nacional de Proteção de Dados (ANPD);
- notificação às instituições financeiras parceiras afetadas;
- notificação aos titulares de dados afetados, quando o incidente possa acarretar risco ou dano relevante.

4 Modelo de resposta a incidentes — cenário de exemplo

Cenário: acesso não autorizado a base de dados de clientes por falha de configuração de sistema.

1. Isolar imediatamente o sistema/ambiente comprometido;
2. Notificar a Equipe de Gestão de Incidentes em até 30 minutos da detecção;
3. Avaliar a extensão do incidente (quais dados, quantos titulares, qual período);
4. Conter o incidente (revogar acessos, corrigir a falha, aplicar patches);
5. Realizar investigação técnica (forense) para identificar causa raiz;
6. Notificar a ANPD e as instituições financeiras parceiras afetadas em até 48 horas, quando aplicável;
7. Notificar os titulares afetados, quando houver risco ou dano relevante a seus direitos;
8. Reforçar controles de segurança (ex.: MFA, revisão de acessos, revisão de configuração);
9. Revisar esta política e os controles técnicos relacionados à luz do incidente ocorrido.

5 Checklist de resposta a incidentes

- ☐ Sistema/ambiente comprometido isolado
- ☐ Equipe de Gestão de Incidentes notificada em até 30 minutos
- ☐ Extensão do incidente avaliada
- ☐ Incidente contido
- ☐ Investigação forense/causa raiz realizada
- ☐ ANPD e parceiros notificados em até 48 horas (quando aplicável)
- ☐ Titulares afetados notificados (quando aplicável)
- ☐ Controles de segurança reforçados
- ☐ Política e controles revisados

6 Referências

- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD);
- ISO/IEC 27005:2018 — Gestão de riscos de segurança da informação.

7 Responsáveis

Papel	Responsável
Autor	Gustavo Schewinski — CTO e DPO

Papel	Responsável
Responsável da área	Gustavo Schewinski — CTO e DPO
Aprovador	Nicolas Ignacio Ryberg — CEO

8 Divulgação

O DPO informará a todos os colaboradores sobre a entrada em vigor deste plano e disponibilizará o documento no repositório interno de políticas da empresa, garantindo que todos saibam como e a quem reportar um incidente.