

# Plano de Resposta a Incidentes

Fluxo de resposta a incidentes de segurança, incluindo comunicação à ANPD e aos titulares.

Obrigatório · Novo - revisar · Atualizado: Julho de 2026

Base legal: Art. 48 e Resolução CD/ANPD nº 15/2024

---

## 1. Definição de incidente

Incidente de segurança: evento adverso confirmado ou com indícios razoáveis que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais, ou que possa acarretar risco ou dano relevante aos titulares.

## 2. Fases de resposta

1. Detecção: alertas de infraestrutura, relatórios internos, titulares ou ANPD.
2. Contenção: revogar acessos, isolar sistemas, rotacionar chaves, preservar evidências.
3. Avaliação: natureza dos dados, volume, titulares afetados, gravidade e probabilidade de dano.
4. Comunicação: ANPD em prazo razoável (orientação: 72h úteis para incidentes graves); titulares quando houver risco relevante.
5. Recuperação: restauração segura, correção de vulnerabilidade.
6. Lições aprendidas: registro do incidente e atualização de controles.

## 3. Equipe e registro

Coordenação: DPO + liderança técnica INFO8.

Todo incidente confirmado gera registro com: data, descrição, dados afetados, medidas adotadas, comunicações realizadas e status de encerramento.