LGPDSense
SOLUÇÕES INTELIGENTES

INCIDENTES E PRIVACIDADE NA LGPD

INCIDENTES E PRIVACIDADE NA LGPD

AUTOR:

LUIS CARLOS BERETA BOTELHO

LGPDSENSE

Introdução

Segurança em ação: incidentes e privacidade

Nos volumes anteriores, vimos como construir uma base sólida para a segurança da informação:

- No **Volume 1**, conhecemos a família ISO/IEC 27000, entendemos a 27001 e a 27002, e traduzimos tudo em **POPs práticos** para o dia a dia da prefeitura.
- No **Volume 2**, demos um passo além, aprendendo a **implementar (27003), medir (27004), avaliar riscos (27005) e auditar (27006 e 27007)**.

Agora, neste **Volume 3**, entramos em uma fase essencial: **como lidar com incidentes e proteger a privacidade dos cidadãos**.

Por que falar de incidentes e privacidade?

Mesmo com controles, políticas e auditorias, incidentes vão acontecer. Pode ser um ataque digital, uma falha humana ou uma vulnerabilidade técnica. O que diferencia uma organização madura é **como ela responde** a esses incidentes.

Além disso, a **LGPD (Lei 13.709/2018)** exige que, quando houver risco relevante, a prefeitura comunique a ocorrência à **ANPD (Autoridade Nacional de Proteção de Dados)** e aos titulares afetados.

Ou seja, não basta corrigir o problema: é preciso **agir com transparência e responsabilidade**.

O papel das normas neste volume

- **ISO/IEC 27035-1:2023** – Ensina a planejar, detectar, responder e aprender com incidentes de segurança da informação.
- **ISO/IEC 29134:2023** – Explica como elaborar o **Relatório de Impacto à Proteção de Dados (RIPD/PIA)**, exigido em muitos casos pela LGPD.

Essas duas normas trazem o equilíbrio entre **ação imediata** (resposta a incidentes) e **planejamento preventivo** (avaliação de impacto).

O que vamos aprender neste volume

Este material está organizado em **sete capítulos**, que unem teoria, prática e exercícios:

1. Entendendo incidentes de segurança da informação (27035).
2. Como planejar e se preparar para incidentes.
3. Resposta prática a incidentes.
4. Lições aprendidas e melhoria contínua.

5. Relatório de Impacto à Proteção de Dados – RIPD/PIA (29134).
6. Casos práticos de incidentes e RIPD no setor público.
7. Exercícios práticos para fixação do aprendizado.

Como usar este material

- Cada capítulo explica os conceitos de forma simples.
- Mostra sua importância legal e prática para a prefeitura.
- Apresenta casos reais adaptados à realidade do serviço público.
- Fecha com checklists para orientar a aplicação imediata.

Assim, você terá não apenas teoria, mas **ferramentas reais para agir diante de crises de segurança e para proteger os dados pessoais do cidadão**.

Se no Volume 1 aprendemos a **construir a base** e no Volume 2 a **medir e auditar**, este Volume 3 é sobre **agir com rapidez e responsabilidade quando algo dá errado** — e sobre **provar que a privacidade está sendo protegida desde o início**.

Capítulo 1 – ISO/IEC 27035

Entendendo os incidentes

O que é isso?

A **ISO/IEC 27035-1:2023** é a norma internacional que ensina como lidar com **incidentes de segurança da informação**.

Ela diferencia dois conceitos:

- **Evento de segurança:** qualquer ocorrência relacionada à segurança (ex.: e-mail suspeito, queda de sistema).
- **Incidente de segurança:** quando o evento realmente compromete a **confidencialidade, integridade ou disponibilidade** das informações.

Em outras palavras: nem todo evento vira incidente, mas todo incidente começa como um evento.

Por que é importante?

Na prefeitura, incidentes podem ocorrer a qualquer momento:

- Um servidor abre um e-mail de phishing.
- Um notebook com dados de beneficiários é perdido.
- O sistema de arrecadação cai em plena época de pagamento.

- Dados de saúde são acessados sem autorização.

Se não houver processo estruturado, cada setor reage de forma improvisada.

Com a ISO 27035, a resposta vira **rotina organizada**: todos sabem como agir, quem acionar e como registrar.

O ciclo de gestão de incidentes (ISO 27035)

1. **Preparação**
    - Criar políticas de resposta a incidentes.
    - Definir responsáveis (TI, DPO, gestores).
    - Disponibilizar formulários e canais de reporte.
2. **Detecção e registro**
    - Servidores relatam eventos suspeitos.
    - Incidentes são registrados formalmente com data, setor e descrição.
3. **Avaliação e classificação**
    - Avaliar gravidade: baixo, médio, alto, crítico.
    - Identificar se envolve dados pessoais (LGPD).

4. **Resposta**
    - Conter o incidente (ex.: isolar computador infectado).
    - Corrigir (ex.: restaurar backup, trocar senhas).
    - Comunicar partes interessadas.
5. **Aprendizado**
    - Produzir relatório final.
    - Extrair lições aprendidas.
    - Atualizar políticas e treinar servidores.

Caso de Uso – E-mail de phishing em secretaria

Um servidor da Secretaria de Administração recebe um e-mail falso solicitando atualização de senha. Ele clica no link e informa suas credenciais.

O que acontece?

- Evento vira incidente: credenciais comprometidas.
- Ação imediata: TI bloqueia conta, redefine senha e verifica acessos suspeitos.
- Comunicação: DPO avalia se houve acesso a dados pessoais.

- Aprendizado: campanha de conscientização reforça cuidado com phishing.

Como aplicar na prática (passo a passo)

1. Criar política de tratamento de incidentes.
2. Treinar servidores para reconhecer eventos suspeitos.
3. Definir canal oficial de registro (formulário ou e-mail institucional).
4. Classificar incidentes por gravidade.
5. Estabelecer fluxo de resposta rápida.
6. Avaliar se o incidente envolve dados pessoais → se sim, comunicar ANPD e titulares.
7. Registrar lições aprendidas em relatório.

Checklist rápido do Capítulo 1

( ) Existe política de tratamento de incidentes.

( ) Servidores sabem como reportar eventos suspeitos.

( ) Há canal oficial de registro de incidentes.

( ) Incidentes são classificados por gravidade.

( ) Fluxo de resposta inclui contenção, correção e comunicação.

( ) Casos envolvendo dados pessoais são comunicados à ANPD e aos titulares.

( ) Lições aprendidas são documentadas e aplicadas.

Assim, a ISO/IEC 27035 mostra que a gestão de incidentes não deve ser improvisada, mas **um processo estruturado e contínuo**, capaz de proteger informações e manter a confiança da população.