LGPDSense
SOLUÇÕES INTELIGENTES

PRÁTICA E GESTÃO DA LGPD

PRÁTICA E GESTÃO
DA LGPD

AUTOR:
LUIS CARLOS BERETA BOTELHO
LGPDSENSE

Introdução

Da prática à gestão: ampliando a segurança da informação

No primeiro volume desta coleção, vimos como os **POPs (Procedimentos Operacionais Padrão)** transformam as orientações da **ISO/IEC 27000, 27001 e 27002** em rotinas claras e aplicáveis para o dia a dia da prefeitura.

Cada servidor pôde entender *o que deve ser feito, por que deve ser feito e como deve ser feito*. Agora, damos um passo além.

Este **Volume 2** é voltado para a **gestão e a maturidade da segurança da informação**: não basta aplicar controles isolados; é preciso **implementar, medir, avaliar riscos e auditar** todo o sistema.

O que muda neste volume?

Se antes o foco eram os POPs práticos, agora o objetivo é compreender as normas que sustentam a **gestão completa de um Sistema de Gestão da Segurança da Informação (SGSI)**:

- **ISO/IEC 27003** – Como implementar um SGSI de forma estruturada.
- **ISO/IEC 27004** – Como medir a eficácia dos controles e gerar indicadores confiáveis.
- **ISO/IEC 27005** – Como identificar e tratar riscos de segurança da informação.

- **ISO/IEC 27006** – Quais são os critérios para certificação em ISO 27001 e como isso impacta órgãos públicos.
- **ISO/IEC 27007** – Como realizar auditorias internas e garantir melhoria contínua.

Por que isso importa para a prefeitura?

Porque a **LGPD (Lei 13.709/2018)** exige mais do que boas intenções: ela exige **provas de conformidade**.

- Métricas (27004) demonstram que controles estão funcionando.
- Gestão de riscos (27005) mostra que a prefeitura está preparada para ameaças.
- Auditorias (27007) comprovam se as práticas estão de acordo com a lei e com a 27001.
- Certificação (27006) pode ser um diferencial de confiança e transparência.

Além disso:

- A **Lei de Governança Digital (Lei 14.129/2021)** reforça a necessidade de eficiência, continuidade e responsabilidade no uso de tecnologias.
- O **Marco Civil da Internet (Lei 12.965/2014)** assegura direitos como privacidade e segurança.

Em outras palavras: aplicar essas normas significa não apenas cumprir a lei, mas **aumentar a confiança do cidadão na gestão pública**.

Como este material está organizado

Este volume foi estruturado em **sete capítulos**, que avançam do planejamento à auditoria:

1. Implementação do SGSI (27003)
2. Métricas e indicadores (27004)
3. Gestão de riscos (27005)
4. Certificação externa (27006)
5. Auditoria interna (27007)
6. Integração com legislações brasileiras
7. Casos práticos de aplicação no setor público

Cada capítulo traz explicação didática, fundamentação legal, exemplos reais, formulários ou checklists para apoiar a prática.

Capítulo 1 – ISO/IEC 27003

Como implementar um SGSI na prática

O que é isso?

A ISO/IEC 27003 é a norma que ajuda organizações a **planejar e implementar** um **Sistema de Gestão da Segurança da Informação (SGSI)** conforme a ISO/IEC 27001.

Se a 27001 diz *"o que deve ser feito"*, a 27003 mostra **como começar**:

- Como estruturar o projeto de segurança da informação.
- Como envolver a alta gestão e os servidores.
- Como definir prioridades, prazos e responsabilidades.

É como o **manual de instruções** para colocar o SGSI de pé.

Por que é importante?

Porque muitas vezes as organizações sabem que precisam se adequar, mas não sabem **por onde começar**. Na prefeitura, isso significa:

- Evitar improvisos na proteção de dados.
- Atender à LGPD de forma organizada.
- Conseguir apoio da gestão e dos servidores.
- Construir uma base sólida para auditorias futuras.

Os passos da ISO/IEC 27003

A 27003 sugere que a implementação do SGSI siga o ciclo **PDCA** (Plan, Do, Check, Act – Planejar, Fazer, Verificar, Agir).

1. **Planejar (Plan)**
    - Definir o escopo: quais áreas e sistemas o SGSI vai abranger (ex.: saúde, arrecadação, folha).
    - Identificar partes interessadas: servidores, cidadãos, fornecedores, ANPD.
    - Definir a política de segurança da informação.
    - Levantar requisitos legais (LGPD, LAI, Marco Civil, etc.).
2. **Executar (Do)**
    - Implementar os controles de segurança definidos na ISO 27001 e detalhados na ISO 27002.
    - Criar POPs e políticas internas.
    - Treinar servidores e gestores.
3. **Verificar (Check)**
    - Medir a eficácia dos controles (aqui entra a ISO 27004).
    - Avaliar se riscos estão sendo tratados (conexão com a ISO 27005).
4. **Agir (Act)**

- Corrigir falhas identificadas em auditorias.
- Melhorar continuamente os processos.

Caso de Uso – Implantação na Secretaria de Saúde

A Secretaria de Saúde da prefeitura decide implementar o SGSI.

- **Planejar**: define que o escopo inicial será apenas os prontuários eletrônicos e sistemas de agendamento.
- **Executar**: cria POPs para gestão de acessos, backup e tratamento de incidentes.
- **Verificar**: mede quantos incidentes de acesso indevido ocorrem em 6 meses.
- **Agir**: ajusta perfis de acesso e reforça treinamento para reduzir os casos.

Resultado: em um ano, o número de incidentes cai drasticamente e a secretaria ganha confiança para ampliar o SGSI para outras áreas.

Como aplicar na prática (passo a passo)

1. Nomear um **responsável** (DPO ou gestor de TI) para coordenar o SGSI.
2. Definir o **escopo inicial** (começar pequeno é melhor do que não começar).
3. Mapear requisitos legais e regulatórios aplicáveis.

4. Elaborar uma **política de segurança da informação** simples e objetiva.
5. Criar um **plano de implementação** com cronograma, responsáveis e entregas.
6. Implantar controles básicos: acessos, backup, tratamento de incidentes.
7. Treinar servidores com POPs e exemplos reais.
8. Avaliar resultados, corrigir falhas e expandir o escopo.

Checklist rápido do Capítulo 1

( ) Existe um responsável nomeado para coordenar o SGSI.

( ) O escopo inicial foi definido (quais áreas e sistemas).

( ) Há uma política de segurança da informação aprovada pela gestão.

( ) Requisitos legais (LGPD, LAI, Marco Civil) foram mapeados.

( ) Há um plano de implementação com prazos e responsáveis.

( ) Servidores receberam treinamento inicial.

( ) Há indicadores básicos para medir resultados.

( ) O ciclo PDCA está em andamento (planejar, fazer, verificar, agir).

Assim, a ISO/IEC 27003 transforma a teoria da 27001 em um **plano de ação estruturado**, permitindo que a prefeitura saia do papel e comece, de fato, a **implantar a segurança da informação de forma organizada**.