LGPDSense
SOLUÇÕES INTELIGENTES

AÇÕES INICIAIS
AS POPS LGPD

AÇÕES INICIAIS

AS POPS DA LGPD

AUTOR:

LUIS CARLOS BERETA BOTELHO

LGPDSENSE

Introdução

ISO 27000, ISO 27001, ISO 27002 e os POPs

A prefeitura lida todos os dias com informações valiosas: dados pessoais de cidadãos, cadastros de saúde, folha de pagamento, sistemas de arrecadação, processos administrativos. Proteger essas informações não é só questão técnica: é uma obrigação legal e um dever com a sociedade.

É nesse cenário que entram as normas da família **ISO/IEC 27000**.

O que é a ISO 27000?

A ISO/IEC 27000 é a norma que abre a série de segurança da informação.
Ela funciona como um **guia introdutório**, estabelecendo:

- **Vocabulário oficial**: define termos como confidencialidade, integridade, disponibilidade, risco, controle e auditoria.
- **Visão geral da série**: mostra como cada norma da família se relaciona, desde a 27001 (requisitos), 27002 (boas práticas), até outras que tratam de riscos, auditoria e incidentes.
- **Base comum de entendimento**: garante que gestores, técnicos e servidores falem a mesma língua quando tratam de segurança da informação.

Em resumo: a ISO 27000 é o **mapa conceitual**. Ela dá o contexto para aplicar corretamente a 27001 e a 27002.

O que é a ISO 27001?

A ISO 27001 é a norma internacional que define os requisitos para criar e manter um Sistema de Gestão da Segurança da Informação (SGSI).

- Ela responde à pergunta: "**O que deve ser feito para proteger informações?**".

- Traz uma visão de gestão: políticas, responsabilidades, controles obrigatórios.
- Exemplo: "A organização deve controlar acessos de usuários" (mas não explica exatamente como).

O que é a ISO 27002?

A ISO 27002 complementa a 27001, servindo como um manual de boas práticas.

- Ela responde à pergunta: "**Como colocar em prática os controles da 27001?**".
- Descreve cada controle com mais detalhes e dá exemplos de aplicação.
- Exemplo: "Senhas devem ter no mínimo 8 caracteres, misturar letras e números, e ser trocadas periodicamente".

Em resumo:

- ISO 27000 = conceitos e visão geral.
- ISO 27001 = o que fazer.
- ISO 27002 = como fazer.

Por que isso é importante para a prefeitura?

- Porque a LGPD (Lei Geral de Proteção de Dados) exige medidas técnicas e administrativas adequadas.
- Porque a Lei de Governança Digital (Lei 14.129/2021) reforça a transparência e a eficiência no uso de tecnologias.
- Porque o Marco Civil da Internet (Lei 12.965/2014) assegura privacidade e segurança na rede.

Aplicar as boas práticas da ISO 27000, 27001 e 27002 significa andar em conformidade com a lei e proteger a confiança do cidadão.

O que são os POPs?

Os Procedimentos Operacionais Padrão (POPs) são a forma de traduzir essas normas em passos simples, claros e aplicáveis no dia a dia da prefeitura.

- Cada POP vira um guia prático para servidores e gestores.
- Enquanto a ISO fala de controles, o POP mostra como executar, com casos de uso, formulários e checklists.

Os 10 POPs deste guia

Este eBook organiza as exigências e boas práticas da ISO 27001 e 27002 em 10 POPs, adaptados à realidade da gestão pública municipal:

1. Gestão de Acessos e Identidades
2. Controle de Ativos de Informação
3. Backup e Recuperação de Dados
4. Tratamento de Incidentes de Segurança
5. Uso Aceitável de Recursos de TI
6. Gestão de Fornecedores e Terceiros
7. Coleta, Armazenamento e Eliminação de Dados Pessoais
8. Atendimento aos Direitos dos Titulares
9. Continuidade de Negócios
10. Treinamento e Conscientização

Como usar este material

- Cada capítulo explica o que é o POP.
- Mostra por que ele é importante, com base na LGPD e nas ISOs.
- Apresenta casos de uso reais da rotina da prefeitura.

- Fornece formulários prontos para impressão.
- Acrescenta as orientações da ISO 27002, traduzidas em linguagem simples.
- Fecha com um checklist rápido para validar a prática.

Assim, o servidor entende o que deve fazer, por que deve fazer e como deve fazer.

CAPÍTULO 1

A família ISO 27000

O que é isso?

A série ISO/IEC 27000 é um conjunto de normas internacionais criadas para ajudar organizações — públicas e privadas — a protegerem suas informações.

Ela funciona como uma **caixa de ferramentas**: cada norma trata de um aspecto da segurança.

- A **ISO 27000** apresenta conceitos e termos básicos.
- A **ISO 27001** define requisitos de gestão.
- A **ISO 27002** traz as boas práticas.
- Outras normas tratam de riscos, auditorias e incidentes.

Por que é importante?

- Dá uma linguagem comum para todos os envolvidos (gestores, técnicos, servidores).
- Mostra que segurança da informação não é só tecnologia, mas envolve pessoas, processos e leis.
- Permite alinhar a prefeitura com padrões internacionais.

Caso de Uso – Comunicação clara

Um servidor da saúde fala em "confidencialidade" e um técnico de TI fala em "controle de acesso". Na prática, estão falando da mesma coisa. A ISO 27000 garante que todos usem os mesmos termos, evitando confusão.

,Checklist rápido:

( ) Sei que a família 27000 é um conjunto de normas, não apenas uma.

( ) Entendi que cada norma cobre uma parte da segurança da informação.

( ) Reconheço que a 27000 é o "guia inicial" da série.

Conceitos fundamentais da ISO 27000

A ISO 27000 define termos-chave que são a base da segurança da informação. Os três pilares são:

1. **Confidencialidade** – apenas pessoas autorizadas acessam a informação.
   Ex.: prontuários médicos só acessíveis a profissionais de saúde.
2. **Integridade** – a informação não pode ser alterada de forma indevida.

Ex.: sistema de arrecadação não pode permitir mudanças em tributos sem registro.

3. **Disponibilidade** – a informação deve estar acessível quando necessária.
   Ex.: o sistema de agendamento de consultas precisa estar online para não prejudicar o cidadão.

Outros conceitos importantes:

- **Controle**: medida que reduz riscos (ex.: senha forte).
- **Risco**: possibilidade de perda ou dano à informação.
- **Incidente**: evento que ameaça dados (ex.: ataque de vírus).

Por que é importante?

Sem esses conceitos claros, a segurança vira um tema nebuloso. Com eles, todos falam a mesma língua.

Caso de Uso – Vazamento de planilha

Uma planilha com CPFs de beneficiários foi enviada sem criptografia.

- Problema de confidencialidade.
- Impacto na integridade (dados podem ser alterados).
- Risco de indisponibilidade (se for perdido).
-

Como a ISO 27000 se conecta à prefeitura

A ISO 27000 mostra que segurança da informação não é apenas um problema técnico, mas também organizacional.

Exemplos práticos na prefeitura:

- Cadastro de alunos → envolve confidencialidade (dados pessoais).
- Folha de pagamento → integridade (valores corretos).
- Protocolo eletrônico → disponibilidade (não pode ficar fora do ar).

Por que é importante?

- A LGPD exige que o setor público proteja dados pessoais.
- O Marco Civil garante privacidade e segurança na internet.
- A Governança Digital cobra eficiência e transparência.

A ISO 27000 fornece a **ponte entre leis brasileiras e práticas internacionais**.

Caso de Uso – Comunicação com a população

Quando ocorre um incidente, a prefeitura precisa informar o cidadão de forma clara. Usar os conceitos da 27000 ajuda a explicar:

- O que aconteceu (incidente).
- Qual o risco.

- Quais medidas foram tomadas (controles).

Questione-se:

( ) Consigo ver a relação da ISO 27000 com a LGPD e outras leis.

( ) Sei que segurança da informação é também uma responsabilidade administrativa.

( ) Entendi como aplicar os conceitos no dia a dia da prefeitura.