

**FACULDADE DE IMPERATRIZ WYDEN – FACIMP WYDEN**  
**WYD6710 - INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**  
**PROFESSOR: THALLES CANELA**

**PLANO BÁSICO DE SEGURANÇA DA INFORMAÇÃO**

**IMPERATRIZ - MA**

**2025**

1. COORDENADOR / EDITOR-CHEFE: WANDERSON MILHOMEM
2. ANALISTA DE AMEAÇAS E VULNERABILIDADES: DONALTH LUCIO
3. ANALISTA DE BOAS PRÁTICAS E GESTÃO DE RISCO: NILTON CÉSAR RODRIGUES NASCIMENTO
4. ANALISTA DE CONTINUIDADE DE NEGÓCIOS: BRUNO DA CRUZ MACIEL

## **PLANO BÁSICO DE SEGURANÇA DA INFORMAÇÃO**

## PLANO BÁSICO DE SEGURANÇA DA INFORMAÇÃO

### Etapa 1: Contexto e Princípios de Segurança da Informação

- **Descrição do cenário :**

“LOJÃO DO ALEMÃO”, é uma empresa de varejo que atua tanto no formato online quanto presencial, oferecendo uma ampla gama de produtos eletrônicos, vestuário e utensílios domésticos. Devido à manipulação de dados sensíveis dos clientes, é essencial implementar um plano de segurança da informação para proteger os dados e garantir a continuidade dos negócios. O sistema de vendas é integrado a bancos de dados que armazenam informações de clientes, transações e inventário.

- **Inventário básico de recursos de TI :**

- Hardware: Servidores para e-commerce, computadores em loja, roteadores, dispositivos de pagamento.
- Software: Sistema de ERP, plataforma de e-commerce, antivírus corporativo, firewalls.
- Redes: VPN para acesso remoto, conexão de lojas com data center.
- Dados Sensíveis: Informações de clientes (CPF, endereço, dados de pagamento), dados financeiros da empresa.

- **Princípios de segurança:**

- Confidencialidade: Proteção dos dados dos clientes por meio de criptografia e controle de acessos.
- Integridade: Uso de assinaturas digitais e checksums para garantir a precisão das transações.
- Disponibilidade: Backup regular e redundância de servidores para evitar interrupções.

- **Mapeamento de possíveis ameaças e vulnerabilidades:**

- Ameaças: Ataques de malware, phishing, roubo de credenciais, fraudes em pagamentos, indisponibilidade de serviço.
- Vulnerabilidades: Falhas de configuração no e-commerce, senhas fracas, falta de monitoramento de logs.

- **Identificação de normas, leis e regulamentações**

- LGPD (Lei Geral de Proteção de Dados): Regula o tratamento de dados pessoais dos clientes.
- ISO 27001: Normas de segurança da informação aplicáveis à empresa.
- PCI-DSS: Padrões de segurança para transações com cartões de crédito.

### Etapa 3: Boas Práticas e Gestão de Risco

- **Boas práticas recomendadas:**

- Uso de autenticação multifator para acesso a sistemas.
- Políticas de senhas fortes e treinamento de colaboradores.
- Implementação de firewall e monitoramento de logs.
- Auditorias regulares de segurança.

- **Estrutura de gestão de risco**

- Avaliação: Identificação de riscos conforme impacto e probabilidade.
- Tratamento: Mitigação de vulnerabilidades.

- Monitoramento: Revisão periódica das medidas de segurança.

#### Etapa 4: Gestão de Continuidade do Negócio

- **Noções de Plano de Continuidade de Negócio (PCN) para o cenário:**
  - ✓ **Identificação de processos críticos;**
    - Funcionamento do e-commerce e lojas físicas.
    - Processamento de pagamentos e emissão de notas fiscais.
  - ✓ **Estratégias de recuperação;**
    - Manutenção de servidores redundantes.
    - Backup diário com armazenamento em nuvem e local.
  - ✓ **Plano de contingência (procedimentos de emergência, responsáveis, comunicação etc.).**
    - Procedimentos de Emergência: Ações imediatas para mitigação de ataques.
    - Responsáveis: Equipe de TI treinada para resposta a incidentes.
    - Comunicação: Plano de notificação para clientes e fornecedores.
- **Bibliografia:**

**O que é um checksum e qual a sua importância na segurança da informação?**

<https://blog.bughunt.com.br/o-que-e-checksum/#:~:text=O%20que%20%C3%A9%20checksum%3F,e%20n%C3%A3o%20foram%20modificados%20indevidamente.>

**E-commerce: o que é, como funciona e como criar?**

<https://www.sydle.com/br/blog/e-commerce-como-funciona-5fca8800725a64268314b75a>

**Chat GPT**

<https://chatgpt.com>