

**Paulo Henrique Luiz do Monte**  
**RA: 82325475**

Professor: Calvetti

## **Atividade 1: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa**

**Empresa Fictícia:** "Delícias da Serra" - Uma pequena empresa de e-commerce que vende produtos artesanais (queijos, doces e cafés) online. A empresa possui 5 funcionários que trabalham de forma híbrida, acessando o sistema de pedidos, a base de clientes e as redes sociais da empresa.

**Documento: Políticas de Segurança da Informação da "Delícias da Serra"**

### **1. Política de Acesso e Controle de Usuários**

- **Política:**
  - **Princípio do Mínimo Privilégio:** Cada funcionário terá acesso apenas aos sistemas e dados estritamente necessários para executar suas funções. Por exemplo, o funcionário de marketing terá acesso às redes sociais, mas não ao sistema financeiro.
  - **Criação e Desativação de Contas:** A criação de novas contas de usuário deve ser formalmente solicitada e aprovada pelo gestor. Contas de ex-funcionários devem ser desativadas imediatamente no último dia de trabalho.
  - **Senhas Fortes:** Todos os usuários devem criar senhas com no mínimo 10 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos. As senhas devem ser trocadas a cada 90 dias.
  - **Autenticação Multifator (MFA):** O acesso ao painel de administração do site e ao sistema de gestão de clientes é obrigatório via MFA (ex: código por aplicativo autenticador).
  - **Revisão de Acessos:** A cada 6 meses, o gestor revisará todos os acessos de usuários para garantir que as permissões continuam adequadas.
- **Justificativa:** Esta política visa garantir que apenas pessoas autorizadas accessem informações sensíveis, como dados de clientes e informações financeiras. O princípio do mínimo privilégio reduz a "superfície de ataque", limitando o dano que uma conta comprometida pode causar. A exigência de

senhas fortes e MFA cria barreiras robustas contra tentativas de acesso não autorizado, protegendo a reputação e os ativos da empresa.

## **2. Política de Uso de Dispositivos Móveis e Redes (BYOD - Bring Your Own Device)**

- **Política:**
  - **Uso Permitido:** Funcionários podem usar seus dispositivos pessoais (notebooks, smartphones) para acessar e-mails corporativos e o sistema de pedidos.
  - **Requisitos Mínimos de Segurança:** Todo dispositivo pessoal que acessa dados da empresa deve ter:
    - Tela de bloqueio com senha, PIN ou biometria.
    - Sistema operacional sempre atualizado.
    - Software antivírus instalado e atualizado (para notebooks).
  - **Redes Seguras:** É proibido acessar sistemas críticos da empresa (como o painel de gestão) a partir de redes Wi-Fi públicas e não seguras (ex: cafés, aeroportos).
  - **Separação de Dados:** Os funcionários devem evitar salvar arquivos com dados de clientes diretamente em seus dispositivos pessoais. O acesso deve ser feito preferencialmente através do portal web seguro da empresa.
  - **Perda ou Roubo:** Em caso de perda ou roubo de um dispositivo, o funcionário deve notificar o gestor imediatamente para que os acessos daquele dispositivo possam ser revogados.
- **Justificativa:** Com o trabalho híbrido, é essencial proteger os dados da empresa que são acessados fora do ambiente físico do escritório. Esta política estabelece um padrão mínimo de segurança para dispositivos pessoais, reduzindo o risco de vazamento de dados por meio de aparelhos perdidos, roubados ou infectados por malware. A restrição ao uso de Wi-Fi público protege contra a interceptação de dados.

## **3. Diretrizes para Resposta a Incidentes de Segurança**

- **Diretrizes:**
  - **Identificação e Notificação:** Qualquer atividade suspeita (ex: e-mail de phishing, lentidão incomum no sistema, alerta de vírus) deve ser imediatamente reportada ao gestor. O funcionário não deve tentar resolver o problema sozinho.
  - **Ação Imediata:** Ao identificar um possível incidente de segurança em seu computador (ex: suspeita de malware), o funcionário deve

- desconectar o dispositivo da rede (cabo ou Wi-Fi) para evitar que a ameaça se espalhe.
- **Análise e Contenção:** O gestor, com apoio de um consultor de TI, irá avaliar a gravidade do incidente, identificar a causa e tomar medidas para conter o dano.
- **Comunicação:** Caso o incidente envolva o vazamento de dados de clientes, a empresa seguirá um plano de comunicação transparente, notificando os afetados conforme exigido pela Lei Geral de Proteção de Dados (LGPD).
- **Pós-Incidente:** Após a resolução, o incidente será documentado para análise, e as políticas de segurança serão revisadas para evitar recorrências.
- **Justificativa:** Um incidente de segurança pode acontecer a qualquer momento. Ter um plano claro de resposta garante que a empresa aja de forma rápida e organizada, minimizando o impacto financeiro e de reputação. A notificação imediata é crucial para conter a ameaça antes que ela se espalhe, e um processo documentado ajuda a aprender com os erros e fortalecer a segurança futura.

#### **4. Política de Backup e Recuperação de Desastres**

- **Política:**
  - **Dados Críticos:** Os dados essenciais para o negócio a serem copiados são: a base de dados de clientes e pedidos, os arquivos do site e as planilhas financeiras.
  - **Frequência:** Backups da base de dados serão realizados automaticamente todos os dias. Backups dos arquivos do site e planilhas serão feitos semanalmente.
  - **Armazenamento (Regra 3-2-1):** Serão mantidas 3 cópias dos dados, em 2 tipos de mídia diferentes, com 1 cópia armazenada fora do local. Na prática:
    - Cópia principal no servidor de hospedagem.
    - Cópia secundária em um HD externo no escritório.
    - Cópia terciária em um serviço de armazenamento em nuvem seguro.
  - **Teste de Recuperação:** A cada três meses, um backup será testado para garantir que os dados podem ser restaurados com sucesso.
- **Justificativa:** A perda de dados pode paralisar as operações da "Delícias da Serra". Seja por uma falha de hardware, um erro humano ou um ataque de ransomware, ter uma rotina de backup robusta garante a continuidade do negócio. A regra 3-2-1 e os testes de recuperação asseguram que, mesmo em

um cenário de desastre, a empresa pode restaurar suas informações e voltar a operar em pouco tempo.

## **Atividade 2: Comparativo de Certificações em Segurança da Informação**

**Certificações Escolhidas:** ISO/IEC 27001 e PCI DSS

**Relatório Comparativo: ISO/IEC 27001 vs. PCI DSS**

### **1. Requisitos para Certificação:**

- **ISO/IEC 27001:** A certificação exige que a organização implemente um **Sistema de Gestão de Segurança da Informação (SGSI)**. O processo é flexível e baseado em risco:
  - A empresa deve definir o escopo do SGSI.
  - Realizar uma análise de riscos completa para identificar ameaças aos seus ativos de informação.
  - Selecionar e implementar controles (sugeridos pela norma ISO 27002/Anexo A) para mitigar os riscos identificados.
  - Criar uma **Declaração de Aplicabilidade (SOA)**, que justifica a escolha (ou não) de cada controle.
  - Passar por auditorias internas e externas para verificar a conformidade e a melhoria contínua do SGSI.
- **PCI DSS (Payment Card Industry Data Security Standard):** A conformidade é baseada em uma abordagem **prescritiva e rígida**.
  - A organização deve implementar obrigatoriamente um conjunto de **12 requisitos principais**, que se desdobram em mais de 300 controles técnicos e operacionais específicos.
  - Os requisitos cobrem áreas como segurança de rede (firewalls), proteção de dados de titulares de cartão (criptografia), gestão de vulnerabilidades (antivírus, patches), controle de acesso rigoroso e monitoramento de redes.
  - A validação da conformidade é feita através de autoavaliações (SAQ) ou auditorias formais por um QSA (Qualified Security Assessor), dependendo do volume de transações da empresa.

## **2. Setores de Atuação:**

- **ISO/IEC 27001:** É uma norma universal e aplicável a **qualquer tipo de organização**, de qualquer tamanho ou setor (tecnologia, saúde, governo, finanças, indústria, etc.). Ela é ideal para empresas que desejam demonstrar um compromisso holístico com a segurança da informação para clientes e parceiros.
- **PCI DSS:** É uma norma de nicho, obrigatória para **qualquer organização que armazena, processa ou transmite dados de cartões de crédito/débito**. Isso inclui lojas (físicas e online), processadores de pagamento, bancos e prestadores de serviços que manuseiam esses dados.

## **3. Benefícios de Obter cada Certificação:**

- **ISO/IEC 27001:**
  - **Vantagem Competitiva:** Demonstra um alto nível de maturidade em segurança, sendo um diferencial em negociações B2B.
  - **Gestão de Riscos Otimizada:** Força a empresa a entender e tratar seus riscos de forma sistemática.
  - **Redução de Incidentes:** Melhora a cultura de segurança e os processos internos, diminuindo a probabilidade de incidentes.
  - **Conformidade Legal:** Ajuda a atender a requisitos de leis como LGPD e GDPR.
- **PCI DSS:**
  - **Permissão para Operar:** É um requisito fundamental para poder aceitar pagamentos com cartão.
  - **Evitar Multas Pesadas:** O não cumprimento pode resultar em multas severas das bandeiras de cartão, além da possível suspensão do direito de processar transações.
  - **Confiança do Consumidor:** Aumenta a confiança dos clientes de que seus dados financeiros estão seguros.
  - **Redução do Risco de Fraude:** A implementação dos controles reduz drasticamente a chance de fraudes e vazamentos de dados de cartão.

## **4. Diferenças na Abordagem de Gestão de Riscos:**

- **ISO/IEC 27001:** Adota uma **abordagem baseada em risco ("risk-based")**. A organização tem autonomia para identificar seus próprios riscos e decidir quais controles são mais adequados para tratá-los. É um modelo flexível, onde a segurança é adaptada à realidade do negócio.
- **PCI DSS:** Adota uma **abordagem prescritiva ("rule-based")**. Os riscos já foram pré-identificados pela indústria de cartões, e a norma dita exatamente quais

controles devem ser implementados para mitigá-los. Não há flexibilidade; a empresa deve seguir as regras à risca, independentemente de sua própria avaliação de risco.

### ***Infográfico Comparativo***

Característica	ISO/IEC 27001	PCI DSS
Foco Principal	Sistema de Gestão de Segurança da Informação (SGSI)	Proteção de Dados de Titulares de Cartão de Pagamento
Setor de Atuação	Universal (Qualquer empresa)	Específico (Quem lida com dados de cartão)
Abordagem	Baseada em Risco (Flexível e adaptativa)	Prescritiva (Rígida e baseada em regras)
Requisito Chave	Implementar um SGSI, analisar riscos e criar uma SOA	Implementar 12 requisitos mandatórios e +300 controles
Benefício Principal	Diferencial competitivo e maturidade em gestão de segurança	Obrigação para processar pagamentos e evitar multas
Escopo	Amplo: Protege todos os ativos de informação da empresa	Restrito: Focado exclusivamente nos dados do cartão