**PRÁTICA 06 – ATIVIDADE 03**

**Relatório comparativo**

**Critérios de Comparação**

1. Requisitos para certificação
2. Empresas que mais utilizam
3. Benefícios de obter a certificação
4. Abordagem de gestão de riscos

**1. Requisitos para Certificação**

|  |  |  |
| --- | --- | --- |
| **Critério** | **ISO 27001** | **PCI DSS** |
| **Foco Principal** | Implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na gestão contínua de riscos. | Proteção de dados de pagamento (cartões de crédito e débito). |
| **Principais Requisitos** | - Avaliação de contexto e riscos - Definição de políticas de segurança - Implementação de controles de segurança - Auditorias e revisões periódicas | - Manter firewall e proteger dados - Criptografia de dados sensíveis - Controle de acessos - Testes e monitoramento contínuos |
| **Flexibilidade** | Altamente flexível; cada organização define seus próprios controles com base nos riscos identificados. | Estrutura rígida com 12 requisitos principais que devem ser seguidos por todas as organizações que processam dados de cartões. |

**2. Empresas que Mais Utilizam**

|  |  |  |
| --- | --- | --- |
| **Critério** | **ISO 27001** | **PCI DSS** |
| **Indústrias** | Empresas de tecnologia da informação, telecomunicações, serviços financeiros, provedores de serviços em nuvem, consultorias de segurança e saúde. | Empresas que lidam com transações de pagamento, como e-commerces, bancos, adquirentes e processadoras de cartões. |
| **Escopo de Aplicação** | Geral, aplicável a qualquer tipo de empresa ou setor que lida com dados sensíveis. | Específico para organizações que armazenam, processam ou transmitem dados de cartões de pagamento. |

**3. Benefícios de Obter a Certificação**

|  |  |  |
| --- | --- | --- |
| **Critério** | **ISO 27001** | **PCI DSS** |
| **Conformidade** | Conformidade com leis globais de proteção de dados (como GDPR e LGPD) e regulamentos de segurança da informação. | Conformidade obrigatória para transações financeiras com cartões, sendo exigida por bandeiras como Visa e Mastercard. |
| **Confiança e Competitividade** | Aumenta a confiança de clientes e parceiros ao demonstrar boas práticas de segurança da informação. | Aumenta a confiança do consumidor ao garantir transações seguras e reduzir o risco de fraudes. |
| **Redução de Riscos** | Melhora a proteção de todos os dados da organização contra vazamentos, ataques cibernéticos e incidentes. | Reduz significativamente os riscos de fraude e vazamento de dados relacionados a cartões de pagamento. |
| **Eficiência Operacional** | Otimiza a segurança e gestão dos dados em geral, com processos bem definidos. | Protege e garante a integridade das operações financeiras, especialmente em transações com cartões. |
| **Reconhecimento Internacional** | Reconhecida globalmente como padrão para a segurança da informação, abrindo portas para negócios internacionais. | Certificação obrigatória para empresas que processam dados de pagamento em todo o mundo. |

**4. Abordagem de Gestão de Riscos**

|  |  |  |
| --- | --- | --- |
| **Critério** | **ISO 27001** | **PCI DSS** |
| **Foco da Gestão de Riscos** | A ISO 27001 tem uma abordagem ampla e contínua de gestão de riscos, que considera todos os ativos da organização (dados, sistemas, infraestrutura). A empresa define sua própria metodologia de análise de riscos e seleciona controles com base nas suas necessidades e contexto. | A PCI DSS tem um foco específico em dados de pagamento. Os requisitos são pré-definidos, com foco na mitigação de riscos relacionados exclusivamente à segurança de transações com cartões de crédito e débito. |
| **Flexibilidade** | Alta flexibilidade: cada organização tem liberdade para identificar e gerenciar riscos de acordo com seu contexto específico. É uma abordagem customizável. | Pouca flexibilidade: os controles são padronizados e devem ser seguidos de maneira rígida para atender às exigências de conformidade. |
| **Abordagem de Melhoria Contínua** | A gestão de riscos é parte integrante do ciclo PDCA (Plan-Do-Check-Act) de melhoria contínua. | A PCI DSS exige revisões e testes contínuos, mas os controles específicos são pré-determinados pela norma. |

**Conclusão**  
A **ISO 27001** é uma norma mais abrangente e flexível, aplicada a diversos tipos de empresas que precisam garantir a segurança da informação em geral, permitindo personalizações na escolha de controles e gestão de riscos. Por outro lado, a **PCI DSS** é mais específica e rígida, focada em proteger os dados de pagamento e é obrigatória para empresas que lidam com cartões de crédito e débito.

As empresas devem escolher entre as duas normas (ou adotar ambas) de acordo com suas necessidades de segurança, tipo de dados que manipulam e exigências regulatórias do setor em que atuam.

**INFOGRÁFICO**

