1. Introdução e Visão Geral

No cenário atual de ameaças cibernéticas, as organizações buscam validar suas posturas

de segurança através de certificações e padrões. Nem todos os padrões são criados da

mesma forma. Este estudo compara dois dos mais influentes, porém fundamentalmente

diferentes, frameworks de segurança: ISO/IEC 27001 e PCI DSS.

Analogia:

• ISO 27001 é como um manual para 'Como construir e gerenciar uma fortaleza segura' —

avalia riscos, projeta políticas e mantém a gestão contínua.

• PCI DSS é um 'Código de Construção de um Cofre de Banco' — prescritivo, com regras

rígidas para proteger um ativo específico (dados de cartão).

2. ISO/IEC 27001: O Padrão-Ouro para Gestão (ISMS)

A ISO/IEC 27001 especifica requisitos para estabelecer, implementar, manter e melhorar

continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Foca na

gestão de risco e na melhoria contínua (PDCA).

3. PCI DSS: A Norma Mandatória para Pagamentos

O PCI DSS (Payment Card Industry Data Security Standard) é um conjunto de requisitos

mandatórios criados pelas bandeiras de cartão e aplicáveis a todas as entidades que

armazenam, processam ou transmitem dados de titulares de cartão (CHD).

4. Estudo Comparativo Detalhado

A tabela a seguir destaca diferenças e semelhanças entre os dois padrões em critérios

selecionados.

Objetivo Principal:

• ISO/IEC 27001: Proteger todas as informações da organização via gestão de risco.

• PCI DSS: Proteger dados de cartão de pagamento (CHD e SAD) contra roubo e fraude.

Escopo:

• ISO/IEC 27001: Flexível e definido pela organização (empresa inteira, departamento ou

processo).

• PCI DSS: Prescritivo e restringe-se ao ambiente de dados do titular do cartão (CDE).

Abordagem:

• ISO/IEC 27001: Baseada em risco; a organização escolhe controles relevantes (Anexo

A).

• PCI DSS: Baseada em regras; checklist de 12 requisitos e centenas de sub-requisitos.

Natureza:

• ISO/IEC 27001: Voluntária (mas frequentemente requerida por clientes).

• PCI DSS: Mandatória para quem processa dados de cartão; não conformidade gera

sanções.

4.1. Requisitos para Certificação

ISO/IEC 27001:

• Implementar um SGSI e definir seu escopo.

• Realizar avaliação de riscos e criar a Declaração de Aplicabilidade (SoA).

• Auditorias em duas fases por órgão certificador credenciado.

• Demonstrar PDCA (melhoria contínua).

PCI DSS:

• Requisitos dependem do volume de transações (Nível 1 a 4).

• Nível 1: Auditoria anual in loco por QSA e Relatório de Conformidade (RoC).

• Níveis 2-4: Questionário de Autoavaliação (SAQ) e evidências de controles.

• Deve demonstrar conformidade com os 12 requisitos aplicáveis.

4.2. Setores de Atuação

ISO/IEC 27001: Universal — tecnologia, saúde, bancos, consultorias e qualquer

organização que queira demonstrar maturidade e conformidade.

PCI DSS: Específico — varejistas, e-commerce, hotéis, companhias aéreas, processadores de pagamento e quaisquer comerciantes que aceitem cartões.

4.3. Benefícios de Obter cada Certificação

Benefícios da ISO 27001:

• Vantagem competitiva em licitações.

• Gestão de risco holística.

• Redução de custos a longo prazo.

• Facilita conformidade com LGPD/GDPR.

Benefícios do PCI DSS:

• Permissão para operar no processamento de cartões.

• Prevenção de multas e sanções das bandeiras.

• Aumenta a confiança do consumidor em meios de pagamento.

4.4. Diferenças na Abordagem de Gestão de Riscos

ISO 27001 (Decida seu Risco): Avalia riscos e permite aceitar, mitigar, transferir ou evitar riscos; flexível e adaptada ao negócio.

PCI DSS (O Risco Já Foi Decidido): Padrão prescritivo que impõe controles sem considerar apetite de risco da organização; conformidade obrigatória.

5. Conclusão

ISO 27001 e PCI DSS são complementares. Uma organização que processa pagamentos idealmente adota ambas: ISO 27001 para a gestão global da segurança e PCI DSS para garantir a conformidade do ambiente de pagamento (CDE).

6. Infográfico Comparativo (instrução)

Sugestão: um infográfico com dois painéis (lado a lado) destacando:

• Escopo: ISO (toda a empresa) vs PCI (dados de cartão).

• Abordagem: Baseada em risco vs Baseada em regras.

• Objetivo: Voluntário/Confiança vs Mandatório/Compliance.