Comparativo entre ISO/IEC 27001 e PCI DSS

Introdução

Com o aumento das ameaças digitais, empresas de todos os setores têm buscado formas de mostrar que levam a segurança da informação a sério. Uma das maneiras de fazer isso é por meio de certificações reconhecidas.

Este material apresenta uma comparação entre dois dos principais modelos de segurança: ISO/IEC 27001 e PCI DSS. Embora ambos sejam importantes, eles têm objetivos e abordagens diferentes.

Uma forma de entender:

- A ISO 27001 funciona como um guia para montar e manter uma estrutura segura — ela ajuda a identificar riscos, criar políticas e manter a segurança como parte da rotina da empresa.
- O PCI DSS é como um manual técnico para proteger cofres — ele traz regras específicas e obrigatórias para proteger dados de cartões de pagamento.

ISO/IEC 27001 – Foco na Gestão da Segurança

A ISO/IEC 27001 define os critérios para criar, aplicar e melhorar continuamente um sistema de gestão voltado à segurança da informação.

Seu foco principal é a análise de riscos e a melhoria constante, seguindo o ciclo PDCA (planejar, executar, verificar e agir).

PCI DSS – Regras para Proteção de Dados de Cartão

O PCI DSS (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento) é um conjunto de exigências criado pelas bandeiras de cartão.

Ele se aplica a qualquer empresa que armazene, processe ou transmita dados de titulares de cartão, como lojas, e-commerces e operadoras de pagamento.

Comparação entre os Padrões

Finalidade

- **ISO/IEC 27001**: Proteger todos os tipos de informação da empresa por meio de gestão de riscos.
- **PCI DSS**: Proteger dados de cartão contra roubo e uso indevido.

Abrangência

- **ISO/IEC 27001**: Pode ser aplicado a toda a empresa ou a áreas específicas, conforme decisão interna.
- **PCI DSS**: Focado apenas no ambiente onde os dados de cartão são tratados.

Forma de Aplicação

- **ISO/IEC 27001**: Baseado em riscos — a empresa escolhe os controles mais adequados.
- **PCI DSS**: Baseado em regras — exige cumprimento de 12 requisitos principais e diversos subitens.

Obrigatoriedade

- **ISO/IEC 27001**: É voluntário, mas muitas vezes solicitado por clientes ou parceiros.
- **PCI DSS**: É obrigatório para empresas que lidam com dados de cartão; o não cumprimento pode gerar penalidades.

Como Obter Cada Certificação

ISO/IEC 27001

- Criar um sistema de gestão de segurança da informação (SGSI) e definir seu escopo.
- Avaliar riscos e elaborar a Declaração de Aplicabilidade.
- Passar por auditorias em duas etapas feitas por uma certificadora autorizada.
- Demonstrar que a empresa segue o ciclo de melhoria contínua (PDCA).

PCI DSS

- Os requisitos variam conforme o volume de transações (classificação de Nível 1 a 4).
- Nível 1: Auditoria presencial anual feita por um especialista credenciado (QSA).
- Níveis 2 a 4: Preenchimento de questionário de autoavaliação e apresentação de evidências.
- A empresa deve comprovar que atende aos 12 requisitos obrigatórios.

Setores que Utilizam

- **ISO/IEC 27001**: Pode ser adotado por qualquer tipo de organização — empresas de tecnologia, saúde, finanças, consultorias, entre outras.

- **PCI DSS**: Voltado para negócios que aceitam pagamentos com cartão — lojas físicas, sites de vendas, hotéis, companhias aéreas e operadoras de pagamento.

Vantagens de Cada Certificação

ISO/IEC 27001

- Melhora a posição da empresa em concorrências e licitações.
- Ajuda a controlar riscos de forma ampla.
- Pode reduzir custos com incidentes de segurança.
- Facilita o cumprimento de leis como LGPD e GDPR.

PCI DSS

- Permite que a empresa continue operando com cartões de pagamento.
- Evita multas e punições das bandeiras.
- Aumenta a confiança dos clientes nos meios de pagamento oferecidos.

Diferenças na Gestão de Riscos

- **ISO 27001**: A empresa avalia seus próprios riscos e decide como lidar com eles — seja aceitando, reduzindo, transferindo ou evitando.
- **PCI DSS**: Os riscos já estão definidos e os controles são obrigatórios, sem espaço para adaptação.

Conclusão

Embora diferentes, ISO 27001 e PCI DSS se complementam.

Empresas que lidam com pagamentos devem considerar a adoção dos dois:

- ISO 27001 para cuidar da segurança como um todo
- PCI DSS para garantir que os dados de cartão sejam protegidos conforme exigido pelas bandeiras

Sugestão Visual

Para facilitar a compreensão, recomenda-se criar um infográfico comparativo com dois painéis lado a lado, destacando:

- Escopo: ISO cobre toda a empresa; PCI foca nos dados de cartão
- Abordagem: ISO é flexível e baseada em riscos; PCI é rígido e baseado em regras

- Objetivo: ISO é voluntário e voltado à confiança; PCI é obrigatório e voltado à conformidade