Estudo Comparativo: ISO/IEC 27001 vs PCI DSS

Introdução

Este relatório apresenta um estudo comparativo entre duas das principais certificações em Segurança da Informação: a ISO/IEC 27001 e a PCI DSS. O objetivo é destacar os requisitos, setores de atuação, benefícios e diferenças na abordagem de gestão de riscos.

1. Requisitos para Certificação

ISO/IEC 27001

• Implementação de um Sistema de Gestão de Segurança da Informação (SGSI).
• Realização de avaliação de riscos.
• Definição e implementação de controles de segurança.
• Auditoria externa e certificação por organismo acreditado.

PCI DSS

• Cumprimento dos 12 requisitos de segurança definidos pelo PCI SSC.
• Proteção de dados de titulares de cartões.
• Manutenção de um ambiente seguro.
• Auditoria anual por QSA (Qualified Security Assessor).

2. Setores de Atuação

ISO/IEC 27001

• Empresas de tecnologia.
• Indústrias.
• Instituições financeiras.
• Órgãos governamentais.
• Prestadores de serviços em geral.

PCI DSS

• Instituições financeiras.
• Empresas de e-commerce.

• Lojas físicas que processam pagamentos com cartão.
• Gateways e processadores de pagamento.

3. Benefícios da Certificação

ISO/IEC 27001

• Reconhecimento internacional.
• Fortalecimento da cultura de segurança.
• Redução de riscos cibernéticos.
• Maior confiança de clientes e parceiros.

PCI DSS

• Redução de riscos de fraudes financeiras.
• Conformidade obrigatória para quem processa cartões.
• Aumento da confiança de consumidores.
• Evita multas e penalidades.

4. Diferenças na Gestão de Riscos

• A ISO/IEC 27001 tem foco amplo na gestão de riscos de segurança da informação, adotando uma abordagem sistemática e baseada em processos.
• A PCI DSS tem foco específico na proteção de dados de cartões de pagamento, com requisitos técnicos bem definidos.

5. Conclusão

Ambas as certificações contribuem para elevar o nível de segurança da informação nas organizações. A ISO/IEC 27001 é mais abrangente e estratégica, adequada para diversos setores. A PCI DSS é mais técnica e obrigatória para empresas que lidam com dados de cartões.

6. Comparativo

Diferenças e similaridades entre as certificações:

Foco Principal

- **ISO/IEC 27001:** Focada na implementação de um **Sistema de Gestão de Segurança da Informação (SGSI)**, abrangendo toda a informação que a empresa considera valiosa.
- **PCI DSS:** Foco estrito e exclusivo na **proteção de dados de portadores de cartão de pagamento** e no ambiente tecnológico onde eles são processados, armazenados ou transmitidos.

Abordagem

- **ISO/IEC 27001:** Adota uma abordagem **baseada em risco (risk-based)**. É flexível, exigindo que a organização identifique seus próprios riscos e selecione os controles de segurança adequados para tratá-los.
- **PCI DSS:** Utiliza uma abordagem **prescritiva (prescriptive)**. É rígida e determina uma lista exata de controles e procedimentos que *devem* ser implementados, sem margem para interpretação.

Escopo

- **ISO/IEC 27001:** O escopo é **definido pela própria organização**. Pode ser aplicado a um único departamento, um produto específico ou à empresa inteira.
- **PCI DSS:** O escopo é **automaticamente definido** por onde os dados de cartão "tocam". Abrange todos os sistemas, processos e pessoas que interagem com o ambiente de dados do titular do cartão (CDE - Cardholder Data Environment).

Aplicabilidade

- **ISO/IEC 27001:** É **universal**. Pode ser adotada por qualquer organização, de qualquer tamanho ou setor (tecnologia, saúde, governo, etc.).
- **PCI DSS:** É **específica**. Aplicável apenas a organizações que processam, armazenam ou transmitem dados de cartões de pagamento.

Motivação para Adoção

- **ISO/IEC 27001:** Geralmente motivada por **vantagem competitiva**, melhoria da gestão de riscos, confiança do cliente e para atender a requisitos de leis de privacidade (como LGPD/GDPR).
- **PCI DSS:** A motivação é uma **obrigação contratual** imposta pelas bandeiras de cartão (Visa, Mastercard, etc.). O principal objetivo é evitar multas pesadas e poder continuar processando pagamentos.

Resultado Final

- **ISO/IEC 27001:** O resultado é uma **certificação** formal, emitida por um organismo credenciado, que atesta a conformidade do sistema de gestão. O certificado é válido por 3 anos, com auditorias de manutenção anuais.
- **PCI DSS:** O resultado é uma **validação de conformidade**, geralmente documentada em um Relatório de Conformidade (ROC) ou um Questionário de Autoavaliação (SAQ). A validação deve ser renovada anualmente.

- **Similaridades a destacar**:

- Ambos buscam reduzir o risco de incidentes de segurança.

- Ambos exigem políticas de segurança claras e definidas.
- Ambos promovem a conscientização e a responsabilidade em segurança da informação.
- Ambos exigem monitoramento e testes contínuos dos controles de segurança.

Elaborado por:
Felipe Pereira do Nascimento - RA: 825126069
Guilherme Dourado Nascimento - RA: 825116419
Bruno de Oliveira Santos - RA: 823223513
Pedro Miranda Rabelo - RA: 825243591
Kauane Sandes Brandão - RA: 825113309
Stephany Ramos Rodrigues - RA: 82512339