

UNIVERSIDADE SÃO JUDAS TADEU - USJT

SISTEMAS COMPUTACIONAIS E SEGURANÇA

EDUARDO IRINEU DE ARAÚJO SANTOS DE SOUZA

FABRÍCIO DOS SANTOS SAMPAIO

JUAN PABLO SILVA DOS SANTOS

LAUANDA JONES ALMEIDA DA SILVA

RAYANNE RAQUEL NASCIMENTO

 KÃUA BARBOSA

**Relatório comparativo - ISO/IEC 27001 vs PCI DSS**

SÃO PAULO

2025

Relatório Comparativo — ISO/IEC 27001 vs PCI DSS

**Objetivo:** Comparar duas certificações/standards de segurança da informação — ISO/IEC 27001 (ISMS) e PCI DSS — cobrindo requisitos, setores de atuação, benefícios e diferenças na abordagem de gestão de riscos. Este documento contém um relatório detalhado e um infográfico pronto para apresentação.

1. **Visão geral curta das normas**

**ISO/IEC 27001**: Padrão internacional para sistemas de gestão de segurança da informação (ISMS). Define requisitos para estabelecer, implementar, manter e melhorar continuamente um ISMS. Aplicável a qualquer setor e tamanho de organização.

**PCI DSS**: Standard criado pelo Payment Card Industry Security Standards Council para proteger dados de titulares de cartão. Contém requisitos técnicos e operacionais detalhados (conhecidos como as 12 exigências principais) e processos de validação de conformidade para comerciantes e provedores de serviços.

1. **Requisitos para certificação**

**ISO/IEC 27001 — requisitos principais**

* Estabelecer o **escopo** do ISMS (limites organizacionais e de informação).
* **Política de segurança** documentada e objetivos de segurança.
* Conduzir **avaliação de riscos** (identificação, análise e avaliação de riscos) e definir **tratamento de riscos**.
* Elaborar e manter um **Statement of Applicability (SoA)** cobrindo controles selecionados.
* Implementar controles (annex A fornece um catálogo de controles; a norma exige controles "necessários" conforme o tratamento de risco).
* **Auditoria interna**, **revisão pela direção** e **auditorias de certificação** por um organismo acreditado (auditoria de etapa 1 e etapa 2; auditorias de vigilância periódicas).
* **Melhoria contínua** através do ciclo PDCA.

**PCI DSS — requisitos principais**

* **Escopo**: identificar e segregar sistemas que armazenam, processam ou transmitem dados de cartão.
* Atender aos requisitos técnicos e operacionais prescritos (agrupados em 12 requisitos, por exemplo: firewall, proteção de dados armazenados, criptografia, gestão de vulnerabilidades, controles de acesso, registros e monitoramento, testes de segurança, políticas).
* **Validação** da conformidade: para grandes provedores/merchants, um Report on Compliance (ROC) por um QSA; para menores, Self-Assessment Questionnaires (SAQs); varreduras trimestrais por Approved Scanning Vendors (ASVs) quando aplicável.
* **Controles contínuos**: scans regulares, testes de penetração, gestão de mudanças e registros de eventos.
* Versões e atualizações: PCI DSS v4.0 (e suas atualizações, como v4.0.1) trouxe maior ênfase em abordagem baseada em risco e opções alternativas de controle.

1. **Setores de atuação**

**ISO/IEC 27001**

* Aplicável a **qualquer organização**: TI, governo, saúde, educação, finanças, manufatura, pequenas e médias empresas, provedores de nuvem, etc.
* Frequentemente adotada por organizações que precisam demonstrar governança de segurança, conformidade regulatória ampla (LGPD/GDPR/SOX), ou ganhar confiança de clientes/partners.

**PCI DSS**

* Aplicável especificamente a qualquer entidade que **processe, transmita ou armazene dados de cartões de pagamento**: comerciantes (e-commerce, lojas físicas), gateways de pagamento, adquirentes, emissores, provedores de serviço (serviços de hospedagem que mantêm ambientes com dados de cartão), provedores de processamento de pagamentos.
* Requisito imposto por contratos com adquirentes e bandeiras (visa, mastercard etc.) — portanto obrigatório para quem lida com cartões.

1. **Benefícios de obter cada certificação**

**Benefícios ISO/IEC 27001**

* Estrutura gerencial reconhecida internacionalmente para proteger ativos de informação.
* Melhora da governança, redução de incidentes e melhor alinhamento com requisitos legais e regulamentares (e.g., LGPD/GDPR).
* Maior confiança de clientes, parceiros e mercado — diferencial comercial.
* Abordagem contínua que promove maturidade e melhoria ao longo do tempo.

**Benefícios PCI DSS**

* Redução direta do risco de vazamento de dados de cartões e fraudes relacionadas.
* Cumprimento de obrigações contratuais com adquirentes e bandeiras; evita multas e penalidades comerciais.
* Validação técnica de controles críticos (firewall, criptografia, gestão de vulnerabilidades) — foco em proteção prática do dado de pagamento.
* Em caso de incidente, estar em conformidade pode reduzir responsabilidades e multas impostas pelas bandeiras.

1. **Diferenças na abordagem de gestão de riscos**

**ISO/IEC 27001 — abordagem baseada em risco e gestão organizacional**

* **Orientação**: gestão de riscos como pilar central. A organização identifica, avalia e trata riscos de acordo com seu contexto e apetite de risco.
* **Flexibilidade**: a norma exige que se selecione controles apropriados com base na avaliação de risco; não impõe controles rígidos (o Anexo A é um catálogo que apoia a seleção).
* **Ciclo contínuo**: integra risco, controles, monitoramento e melhoria contínua (PDCA).
* **Escopo amplo**: não só tecnologia — também pessoas, processos e ativos físicos.

**PCI DSS — abordagem prescritiva com elementos de risco**

* **Orientação**: fortemente prescritiva em requisitos técnicos-operacionais que devem ser implementados para proteger dados de cartão.
* **Validação**: além de executar controles, é necessário validar sua eficácia periodicamente (scans ASV, ROCs, SAQs, testes de penetração).
* **Evolução para risco**: versões recentes (v4.0) introduzem maior flexibilidade e opções baseadas em risco (Customized Approach), mas ainda mantêm requisitos mandatórios e validação rigorosa.
* **Foco**: proteger especificamente o fluxo de dados de pagamento; menos ênfase em governança geral, maior ênfase em controles técnicos e evidências verificáveis.