**ATIVIDADE 2 — Estudo Comparativo de Certificações**

Certificações escolhidas: **ISO/IEC 27001** × **PCI DSS**

**Quadro Comparativo**

| **Critério** | **ISO/IEC 27001** | **PCI DSS** |
| --- | --- | --- |
| **O que é?** | Norma internacional de SGSI (Sistema de Gestão de Segurança da Informação) | Padrão de segurança para processamento de cartões de pagamento |
| **Requisitos para certificação** | Implementação de SGSI, análise de riscos, controles ISO 27002, auditorias periódicas | Atender 12 requisitos específicos (como criptografia, controle de acesso, teste de rede) e auditoria anual |
| **Setores que utilizam** | Qualquer setor: saúde, educação, indústria, tecnologia | Bancos, e-commerce, adquirentes, empresas que processam cartões |
| **Benefícios principais** | Confiança do mercado, vantagem competitiva, gestão de riscos estruturada | Prevenção de fraudes, obrigatória para quem processa cartões, evita multas |
| **Abordagem de Riscos** | Baseada em **gestão de riscos** contínua e personalizada ao negócio | Controle prescritivo focado em **risco financeiro e antifraude** |
| **Escopo** | Toda a organização | Só o ambiente que lida com cartões |

**Similaridades**

* Ambas melhoram a postura de segurança da organização
* Exigem controles técnicos e administrativos
* Requerem auditorias e conformidade contínua

**Diferenças-chave (resumo)**

| **ISO/IEC 27001** | **PCI DSS** |
| --- | --- |
| Flexível e aplicável a qualquer tipo de organização | Específica para pagamento eletrônico |
| Baseada na gestão e mitigação contínua de riscos | Requisitos mais rígidos e prescritivos |
| Certificação voluntária | Pode ser obrigatória por contrato no setor financeiro |