Atividade 2 – Comparativo de Certificações em Segurança da Informação

Certificações Escolhidas

- **ISO/IEC 27001**
- **PCI DSS (Payment Card Industry Data Security Standard)**

1. Requisitos para Certificação

Item	ISO/IEC 27001	PCI DSS
Foco principal	Sistema de Gestão de Segurança da Informação (SGSI)	Proteção de dados de cartão de crédito
Requisitos	Política, gestão de riscos, controles, auditoria e melhoria contínua	12 requisitos técnicos e operacionais para segurança de dados
Tipo de certificação	Organizacional	Organizacional e técnica
Validação	Auditorias periódicas independentes	Auditorias e testes de conformidade anuais

2. Setores de Atuação

- **ISO/IEC 27001:** Qualquer empresa que lide com dados sensíveis (TI, saúde, educação, governo).
- **PCI DSS:** Indústrias financeiras, e-commerces e instituições que processam cartões de pagamento.

3. Benefícios

Benefício	ISO/IEC 27001	PCI DSS
Fortalece confiança dos clientes	✅	✅

Reduz riscos de incidentes de segurança	✅	✅
Exigência de parceiros e contratos	✅	✅
Melhora governança e gestão de riscos	✅	Parcial
Atende exigências legais (LGPD, etc.)	✅	✅

4. Diferenças na Abordagem de Gestão de Riscos

- **ISO/IEC 27001:** Baseada na identificação e tratamento sistemático de riscos.
- **PCI DSS:** Baseada em controles técnicos e monitoramento constante de sistemas de pagamento.

Conclusão

Ambas as certificações são complementares.
A **ISO/IEC 27001** é mais ampla e estratégica, ideal para organizações que desejam uma cultura de segurança.
A **PCI DSS** é mais técnica e obrigatória para quem processa pagamentos com cartão.
Empresas que adotam ambas demonstram alto nível de maturidade em segurança da informação.