Universidade São Judas Tadeu

Eduardo Cecilio Alves Santos – RA:824224719

Ian Bastos Leme de Moraes – RA:825111187

Kauan Camargo – RA: 825141414

Lucas Tosta Piola – RA:825137169

Victor Volpi – RA:825117218

Wagner Quispe Espinal – RA:823154959

Relatório Comparativo: ISO/IEC 27001 - PCI DSS

1. Requisitos para Certificação

ISO/IEC 27001:

- Define requisitos para estabelecer, implementar, manter e melhorar um **Sistema de Gestão de Segurança da Informação (SGSI)**.
- Exige uma **análise de riscos personalizada**, definição de controles com base em riscos, e o envolvimento da alta direção.
- Auditoria por organismo certificador acreditado.
- Baseada em normas internacionais e aplicável a qualquer tipo de organização.

PCI DSS (Payment Card Industry Data Security Standard):

- É um **padrão de segurança da indústria de cartões de pagamento**.
- Define **requisitos técnicos e operacionais** obrigatórios para qualquer organização que armazene, processe ou transmita dados de cartões de crédito.
- Avaliação feita por um **Qualified Security Assessor (QSA)** ou autoavaliação (SAQ), dependendo do volume de transações.
- Não é uma norma internacional, mas é obrigatória para empresas que operam com dados de pagamento.

2. Setores de Atuação

- **ISO/IEC 27001**:
  Aplicável a **qualquer organização**, de qualquer setor, que deseje proteger suas informações: saúde, governo, TI, educação, manufatura etc.
- **PCI DSS**:

Específico para empresas **que lidam com dados de cartões de pagamento**, como e-commerces, bancos, fintechs, varejistas e gateways de pagamento.

3. Benefícios de Obter Cada Certificação

- **ISO/IEC 27001**:
  - Melhoria contínua da segurança da informação.
  - Fortalecimento da **governança corporativa**.
  - **Reconhecimento internacional** e vantagem competitiva.
  - Confiança aumentada com clientes, parceiros e stakeholders.

- **PCI DSS**:
  - Redução do risco de **fraude e vazamento de dados de pagamento**.
  - Cumprimento obrigatório para continuar operando com cartões.
  - Evita multas e sanções dos consórcios de cartão.
  - Melhoria nos controles técnicos e operacionais específicos de pagamento.

4. Diferenças na Abordagem de Gestão de Riscos

- **ISO/IEC 27001**:
  - Gestão de riscos é **central**, com análise e tratamento baseados no contexto e objetivos da organização.
  - Envolve identificação, avaliação, e tratamento de riscos de forma **flexível e contínua**.
  - Permite adaptação de controles de segurança conforme o perfil da empresa.

- **PCI DSS**:
  - Foco em controles **padronizados e mandatórios**.
  - A gestão de riscos é **implícita**, não há um processo formal como no ISO 27001.
  - Requisitos são os mesmos independentemente do contexto da empresa.

Comparação ISO/IEC 27001 vs PCI DSS

	ISO/IEC 27001	PCI DSS
Aplicação	Universal (todos os setores)	Dados de cartões de pagamento
		Requisitos técnicos e operacionais obrigatórios
	SGSI + análise de risco personalizada	Obrigatória (se lida com cartões), via QSA ou SAQ
Certificação	Voluntária, por órgão acreditado	Implícita e padronizada
Gestão de Riscos	Reconhecimento global governança, confiança	Redução de fraudes, conformidade com bandeiras
Foco	Segurança da informação como um todo	Segurança de dados de cartão de pagamento