Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Profº Robson Calvetti

Lucas Gabriel Hora Benetti - 825134041

Aula 6 - Atividade 2

Comparativo de Certificações em Segurança da Informação: ISO/IEC 27001 vs. PCI DSS

ISO/IEC 27001

Requisitos para Certificação

- Exige o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão da Segurança da Informação (SGSI).
- Os requisitos incluem definir o Contexto da organização, Liderança e compromisso, Planejamento para gerenciamento de riscos e Alocação de recursos.
- Requer a implementação de controles de segurança com base em uma avaliação de riscos e a elaboração de uma Declaração de Aplicabilidade (SOA).

Setores de Atuação

- É voltada a organizações de todos os tamanhos e tipos.
- É aplicável a qualquer empresa que lide com informações e queira proteger sua propriedade intelectual, dados de processo e resultados de serviços.
- Setores como tecnologia, finanças, telecomunicações, saúde e governamental utilizam esta norma.

Benefícios

- Garante uma gestão eficaz de todo o ciclo de vida da informação por meio de uma abordagem baseada em risco.
- Fortalece a imagem da empresa e a confiança dos clientes, demonstrando compromisso com a proteção de dados.
- Ajuda a organização a cumprir obrigações legais e regulatórias (como LGPD e GDPR).
- Proporciona um diferencial competitivo e melhorias nas relações B2B e B2C.

Abordagem de Gestão de Riscos

- Abordagem é **baseada em risco e flexível**.
- Exige que a organização adapte medidas e políticas de segurança exclusivas para a realidade do seu negócio.
- O foco principal é no processo de gestão (SGSI) para seleção sistemática de controles de segurança.

PCI DSS (Payment Card Industry Data Security Standard)

Requisitos para Certificação

- Define 12 requisitos principais de segurança que devem ser implementados.
- Os requisitos incluem o uso de *firewalls*, criptografia de dados em trânsito e em repouso, e controle de acesso baseado em privilégio mínimo.
- Exige testes regulares de segurança e a manutenção de uma política de segurança para todo o pessoal.
- A conformidade deve ser validada anualmente.

Setores de Atuação

- É um padrão de segurança para o setor de cartões de crédito.
- É obrigatório para qualquer entidade que armazene, processe ou transmita dados de titulares de cartão de pagamento.
- Aplica-se a *e-commerce*, varejo digital, processadoras de pagamento e prestadores de serviços que manipulam dados de cartão.

Benefícios

- Seu principal objetivo é reduzir os riscos de ataques, comprometimento das informações e fraudes relacionadas a dados de cartão.
- É essencial e obrigatório para operar legalmente no ecossistema de pagamentos com cartão.
- Ajuda a fortalecer a reputação da marca e a confiança dos clientes ao proteger informações sensíveis de cartão de crédito.

Abordagem de Gestão de Riscos

- Abordagem é mais **prescritiva**.
- Define um conjunto específico de controles técnicos e organizacionais que devem ser implementados para garantir a proteção dos dados.
- O foco é na implementação dos controles definidos no padrão para mitigar o risco de vazamento de dados de cartão.

Similaridades (Destaque)

- Ambos têm como objetivo principal proteger ativamente a segurança da informação.
- Ambos requerem o uso de controles técnicos e organizacionais, como controle de acesso e políticas de segurança, para garantir a confidencialidade, integridade e disponibilidade das informações sensíveis.
- O SGSI da ISO/IEC 27001 pode ser usado como uma estrutura para ajudar a alcançar a conformidade com o PCI DSS.

Infográfico