USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti – Atividade 2

GRUPO: Acácio, Daniel Silva, Matheus Bolato, Munir

ATIVIDADE 2:

O grupo deve escolher duas certificações de segurança da informação (por exemplo, ISO/IEC 27001 e PCI DSS) e fazer um estudo comparativo; deve ser abordado: Requisitos para certificação; setores de atuação (em que tipo de empresas ou indústrias cada certificação é mais usada); benefícios de obter cada certificação; diferenças na abordagem de gestão de riscos.

Comparativo de Certificações em Segurança da Informação

ISO/IEC 27001 e PCI DSS são duas das certificações de segurança da informação mais importantes, mas têm escopos, requisitos e abordagens diferentes. A principal distinção é que a ISO 27001 é um padrão internacional para um sistema de gestão de segurança da informação (SGSI) geral, enquanto o PCI DSS é um padrão mandatório e prescritivo, focado especificamente em proteger dados de cartões de pagamento.

Requisitos para certificação

Característica	ISO/IEC 27001	PCI DSS
Escopo	A organização define o escopo do seu SGSI, que pode cobrir toda a empresa ou partes específicas, como um produto ou departamento. O escopo é flexível e adaptado à necessidade do negócio.	O escopo se restringe a qualquer ambiente que armazene, processe ou transmita dados de titulares de cartão (chamado de CDE – *Cardholder Data Environment*).
Requisitos	Exige o estabelecimento e a manutenção de um SGSI baseado no ciclo PDCA (Planejar, Fazer, Checar e Agir). Os controles de segurança são definidos com base na análise de risco da organização.	Requer a implementação de 12 requisitos específicos e cerca de 250 controles, como a construção de redes seguras, proteção de dados do titular do cartão, gestão de vulnerabilidades e controle de acessos.
Natureza	O framework é baseado em riscos, o que significa que a empresa tem flexibilidade para escolher e implementar os controles de segurança mais adequados ao seu contexto.	É um padrão altamente prescritivo e baseado em regras. As empresas devem implementar os controles de segurança exigidos, sem muita margem de manobra.
Obrigatoriedade	É uma certificação voluntária. A obtenção e a manutenção dependem do interesse estratégico da organização ou de exigências contratuais.	É mandatório para todas as empresas que lidam com dados de cartão de crédito, sendo uma exigência dos emissores de cartão (Visa, Mastercard, etc.).
Certificação	A certificação é voluntária e realizada por um órgão externo credenciado, após uma auditoria que verifica a conformidade com o SGSI.	O processo de validação é mandatório para todas as empresas que lidam com dados de cartão. A auditoria é realizada por um Assessor de Segurança Qualificado (QSA).

Setores de atuação

Característica	ISO/IEC 27001	PCI DSS
Setores	Aplica-se a qualquer tipo de organização, de qualquer tamanho e de qualquer setor, que queira gerenciar a segurança da informação de forma sistemática. É frequentemente adotada em setores como tecnologia, saúde, finanças e setor público.	Aplica-se a todas as empresas, de qualquer setor, que aceitam, processam, armazenam ou transmitem dados de cartões de pagamento. Isso inclui varejistas, provedores de serviço de pagamento, instituições financeiras, e-commerce e call centers.

Benefícios de obter cada certificação

Característica	ISO/IEC 27001	PCI DSS
Governança de TI	Fornece uma abordagem estruturada para a segurança da informação, melhorando a gestão de riscos e a tomada de decisões.	Ajuda a melhorar a segurança de redes e sistemas, protegendo o ambiente de dados de cartão de crédito.
Credibilidade	Reconhecimento internacional que aumenta a confiança de clientes, parceiros e fornecedores. É um diferencial competitivo.	Conformidade obrigatória que garante a continuidade dos negócios, mantendo a capacidade de processar transações com cartão.
Continuidade	O modelo PDCA promove a melhoria contínua da segurança, tornando a organização mais resiliente a ameaças.	Evita multas e sanções impostas pelos emissores de cartão em caso de não conformidade ou violação de dados.
Abrangência	Cria um SGSI abrangente que protege todos os tipos de informações e ativos, não apenas os dados mais sensíveis.	Protege especificamente os dados de cartões, um ativo crítico e alvo frequente de ataques cibernéticos.

Diferenças na abordagem de gestão de riscos

Característica	ISO/IEC 27001	PCI DSS
Metodologia	O cerne da certificação é a gestão de riscos. A organização identifica, avalia e trata os riscos de segurança de acordo com sua tolerância a riscos e objetivos de negócio.	O gerenciamento de riscos é menos central. Embora exija avaliações de risco contínuas, a conformidade é garantida pela implementação dos requisitos técnicos e operacionais já estabelecidos pelo padrão.
Flexibilidade	Oferece mais flexibilidade. Permite que a organização adapte os controles de segurança para abordar os riscos identificados no seu contexto específico, desde que justifique suas decisões.	É menos flexível e mais rigoroso. Impõe controles e procedimentos específicos, com pouca margem para customização, pois o objetivo é atender aos requisitos de segurança da indústria de cartões.
Foco	O foco é na gestão do processo e do sistema de segurança, assegurando a melhoria contínua e a adequação do SGSI.	O foco é na conformidade com os requisitos pré-definidos para proteger os dados do titular do cartão, garantindo que o ambiente de pagamento seja seguro.