Atividade 02

Prática 06

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

1. Requisitos para Certificação

ISO/IEC 27001:

- Sistema de Gestão de Segurança da Informação (SGSI): A organização deve estabelecer, implementar, manter e melhorar continuamente um SGSI.

- Avaliação de Riscos: Identificação e avaliação de riscos à segurança da informação.

- Documentação: Criação de uma documentação que inclua política de segurança da informação, objetivos, e controles implementados.

- Auditorias Internas: Realização de auditorias internas regulares para garantir a conformidade e eficácia do SGSI.

- Revisão pela Direção: Revisão do SGSI pela alta direção para assegurar a adequação e eficácia.

PCI DSS:

- Proteção de Dados de Cartão: Requisitos específicos para proteger os dados dos cartões de pagamento.

- Segurança da Rede: Implementação de firewalls, criptografia, e proteção de sistemas.

- Gestão de Vulnerabilidades: Identificação e correção de vulnerabilidades de sistemas e software.

- Controle de Acesso: Limitação do acesso a dados de cartão apenas a pessoas autorizadas.

- Monitoramento e Testes: Monitoramento de acesso à rede e testes regulares de segurança.

2. Setores de Atuação

ISO/IEC 27001

- Indústrias de TI: Empresas de tecnologia que lidam com dados sensíveis.

- Serviços Financeiros: Bancos e instituições financeiras que necessitam de proteção de dados.

- Saúde: Organizações que gerenciam informações de saúde e dados pessoais.

- Governo: Entidades governamentais que precisam garantir a confidencialidade e integridade das informações.

PCI DSS

- Varejo: Lojas físicas e online que processam pagamentos com cartão.

- Instituições Financeiras: Bancos e empresas de pagamento que processam transações de cartão.

- Serviços de E-commerce : Plataformas que facilitam transações de pagamento online.

- Hospitalidade: Hotéis e restaurantes que aceitam pagamentos com cartão.

3. Benefícios de Obter Cada Certificação

ISO/IEC 27001

- Reconhecimento Internacional: A certificação é reconhecida mundialmente, aumentando a credibilidade da organização.

- Melhoria na Gestão de Riscos: Ajuda a identificar, gerenciar e mitigar riscos associados à segurança da informação.

- Conformidade Regulamentar: Facilita a conformidade com legislações e regulamentações de proteção de dados.

- Aumento da Confiança: Garante aos clientes que seus dados estão sendo geridos de forma segura.

PCI DSS

- Proteção de Dados de Clientes : Reduz o risco de violação de dados e fraudes financeiras.

- Aumento da Confiança do Consumidor: Demonstra compromisso com a segurança dos dados dos clientes.

- Evita Multas: Estar em conformidade com PCI DSS ajuda a evitar penalidades financeiras significativas em caso de violação.

- Melhoria em Processos de Pagamento: Melhora a segurança e a eficiência das transações financeiras.

4. Diferenças na Abordagem de Gestão de Riscos

ISO/IEC 27001

- Abordagem Abrangente : Foca na gestão de riscos de maneira holística, abrangendo todos os aspectos da segurança da informação.

- Ciclo de PDCA: Utiliza o ciclo Plan-Do-Check-Act (PDCA) para a melhoria contínua do SGSI.

- Envolvimento da Alta Direção : A gestão de riscos é frequentemente revisada e aprovada pela alta direção, garantindo compromisso em todos os níveis.

PCI DSS

- Foco em Dados de Cartão: A abordagem é mais restrita, com foco específico na proteção de dados de cartões de pagamento.

- Requisitos Prescritivos : Os requisitos são diretos e prescritivos, exigindo que as organizações implementem controles específicos para atender aos padrões.

- Auditorias Regulares: Exige auditorias frequentes para garantir que as medidas de segurança estão em vigor e funcionando corretamente.

Conclusão

Ambas as certificações, ISO/IEC 27001 e PCI DSS, são cruciais para a segurança da informação, mas atendem a propósitos e necessidades diferentes. A ISO/IEC 27001 é mais abrangente e focada na gestão de riscos em geral, enquanto o PCI DSS é específico para o setor de pagamentos e proteção de dados de cartões. A escolha entre elas deve ser baseada nos objetivos de segurança da informação da organização e no setor em que opera.

ATIVIDADE DO CALVETTI

ISO/IEC 27001

Sistema de Gestão de Segurança da Informação (SGSI), Avaliação de Riscos, Documentação,Auditorias Internas,Revisão pela Direção

PCI DSS

Proteção de Dados de Cartão, Segurança da Rede, Gestão de Vulnerabilidades, Controle de Acesso, Monitoramento e Testes.

SETORES DE ATUAÇÃO

Indústrias de TI,Serviços Financeiros, Saúde,Governo.

SETORES DE ATUAÇÃO

Varejo, Instituições Financeiras, Serviços de E-commerce, Hospitalidade.

BENEFÍCIOS DE OBTER CADA CERTIFICAÇÃO

Reconhecimento Internacional, Melhoria na Gestão de Riscos, Conformidade Regulamentar, Aumento da Confiança.

BENEFÍCIOS DE OBTER CADA CERTIFICAÇÃO

Proteção de Dados de Clientes, Aumento da Confiança do Consumidor, Evita Multas, Melhoria em Processos de Pagamento.

DIFERENÇAS NA ABORDAGEM DE GESTÃO DE RISCOS

Abordagem Abrangente, Ciclo de PDCA, Envolvimento da Alta Direção.

DIFERENÇAS NA ABORDAGEM DE GESTÃO DE RISCOS

Foco em Dados de Cartão, Requisitos Prescritivos, Auditorias Regulares.