Integrantes Do Grupo

Otavio Paiva/ RA: 824147017
Gabriel Prieto/ RA: 824142064
Eduardo Baptistella/ RA: 824147595

Relatório Comparativo: ISO/IEC 27001 vs PCI DSS

Requisitos para Certificação

ISO/IEC 27001

Objetivo: A ISO/IEC 27001 é uma norma internacional que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Ela visa estabelecer, implementar, manter e melhorar a segurança da informação dentro de uma organização.

Requisitos principais:

Política de segurança da informação: A organização deve ter uma política clara de segurança.

Gestão de riscos: Identificação e avaliação de riscos relacionados à segurança da informação.

Controles de segurança: Implementação de controles específicos (mais de 100 controles sugeridos na norma).

Plano de ação: A organização deve demonstrar como responde a incidentes de segurança.

Auditoria e revisão: Auditorias internas regulares e revisão pela direção.

PCI DSS (Payment Card Industry Data Security Standard)

Objetivo: O PCI DSS é um conjunto de requisitos de segurança para proteger os dados de cartão de pagamento. A certificação visa garantir que as organizações que armazenam, processam ou transmitem dados de cartões de crédito e débito sigam práticas de segurança rigorosas.

Requisitos principais:

Segurança de rede e sistemas: Implementação de firewalls, roteadores e medidas de segurança para proteger os dados.

Criptografia: Criptografia de dados sensíveis, como números de cartão.

Acesso restrito: Controle rigoroso sobre quem pode acessar dados sensíveis.

Monitoramento e testes: Monitoramento contínuo dos sistemas e testes de segurança.

Gestão de vulnerabilidades: Implementação de controles contra vulnerabilidades e patching de sistemas.

Política de segurança: Documento que descreve as práticas e políticas de segurança de dados.

2. Setores de Atuação

ISO/IEC 27001

Setores: A ISO/IEC 27001 é aplicável a qualquer tipo de organização, independentemente de seu porte ou setor. É utilizada globalmente em setores como:

Tecnologia da Informação: Empresas de software e provedores de serviços de TI.

Saúde: Hospitais e clínicas que lidam com informações sensíveis dos pacientes.

Financeiro: Bancos e seguradoras que precisam proteger dados financeiros.

Governo e Defesa: Organizações públicas que precisam garantir a confidencialidade e integridade das informações governamentais.

Indústria: Empresas que gerenciam dados sensíveis relacionados à manufatura ou à cadeia de suprimentos.

PCI DSS

Setores: O PCI DSS é especificamente voltado para empresas que lidam com cartões de pagamento, e está mais restrito a indústrias como:

Varejo: Lojas físicas e online que aceitam pagamentos com cartão.

Financeiro: Bancos, processadores de pagamento, adquirentes de cartões e instituições que armazenam ou processam dados de cartões de crédito.

E-commerce: Plataformas de comércio eletrônico que processam transações com cartões.

Empresas de processamento de pagamento: Empresas que lidam diretamente com transações de cartões de crédito, como gateways de pagamento e processadores de cartões.

3. Benefícios de Obter Cada Certificação

ISO/IEC 27001

Proteção aprimorada de dados e ativos de informação contra ameaças internas e externas.

Redução de riscos: Identificação e mitigação de riscos à segurança da informação de forma contínua.

Melhoria da confiança: Prova de compromisso com a segurança da informação para clientes, parceiros e partes interessadas.

Compliance regulatório: Auxilia no cumprimento de regulamentações como GDPR, HIPAA e outras leis de proteção de dados.Vantagem competitiva: A certificação ISO/IEC 27001 pode ser um diferencial em mercados onde a segurança é uma prioridade.

PCI DSS

Segurança de dados de pagamento: Protege informações sensíveis de cartões de crédito e débito.

Evita multas: Não conformidade com PCI DSS pode resultar em multas pesadas e danos à reputação da empresa.

Confiança do cliente: Demonstra que a organização segue as melhores práticas de segurança no processamento de dados financeiros.

Proteção contra fraudes: Reduz o risco de fraudes e acessos não autorizados aos dados de pagamento.

Acesso a novos mercados: Empresas certificadas podem expandir sua atuação em mercados internacionais que exigem PCI DSS.

4. Diferenças na Abordagem de Gestão de Riscos

ISO/IEC 27001

Gestão de riscos baseada no SGSI: A ISO/IEC 27001 adota uma abordagem holística e contínua para gestão de riscos, abrangendo todos os aspectos da segurança da informação dentro da organização.

Risco organizacional: A gestão de riscos considera os riscos globais que a organização enfrenta em relação à proteção de informações, incluindo ativos de TI, pessoas, processos e políticas.

Avaliação contínua: A gestão de riscos deve ser revisada e ajustada regularmente com base em auditorias internas, análises de ameaças e mudanças no ambiente organizacional.

PCI DSS

Gestão de riscos focada em dados de pagamento: A abordagem do PCI DSS é mais específica e voltada para a proteção dos dados sensíveis de cartões de pagamento. A gestão de riscos está mais voltada para proteger transações e a infraestrutura de pagamento.

Controles técnicos e operacionais: Os controles de segurança se concentram em tecnologias específicas para proteger os dados de pagamento, como criptografia, controle de acesso e monitoramento de sistemas.

Foco na conformidade regulatória: O foco está em atender aos requisitos de segurança para garantir a conformidade com o padrão PCI, em vez de uma abordagem abrangente de gestão de riscos para toda a organização.

Infográfico: Comparativo entre ISO/IEC 27001 e PCI DSS

[Infográfico]

O infográfico a seguir destaca as principais diferenças e semelhanças entre as certificações ISO/IEC 27001 e PCI DSS.

Aspecto	ISO/IEC 27001	PCI DSS
Objetivo	Gestão de Segurança da Informação	Proteção de Dados de Cartões de Pagamento
Setor de Atuação	Geral (todos os setores)	Setores de Pagamentos e Financeiros
Abrangência de Riscos	Riscos gerais de segurança da informação	Focado em dados de pagamento e transações
Número de Requisitos	Mais de 100 controles e práticas	12 requisitos principais
Tipo de Certificação	Abrange toda a organização	Específico para empresas de pagamento
Frequência de Auditoria	Auditorias anuais ou periódicas	Auditorias anuais

Benefícios	Proteção de dados e confiança geral	Proteção de dados de pagamento e compliance
Exemplo de Empresas	Qualquer organização	Empresas que processam dados de cartões