ISO 27001 vs PCI DSS

Entenda as diferenças e similaridades entre ISO/IEC 27001 e PCI DSS, dois padrões importantes para segurança da informação.

1

Objetivo

ISO 27001: Estabelecer um Sistema de Gestão de Segurança da Informação (SGSI). PCI DSS: Proteger dados de cartão de crédito.

2

Âmbito

ISO 27001: Aplicável a qualquer organização. PCI DSS: Aplicável a empresas que processam dados de cartão de crédito.

3

Requisitos

ISO 27001: Mais abrangente, com requisitos gerais para SGSI. PCI DSS: Focado em segurança de dados de cartão de crédito.

4

Aplicações

ISO 27001: Mais ampla, incluindo proteção de dados confidenciais. PCI DSS: Específica para dados de cartão de crédito.

5

Similaridades

Ambos os padrões enfatizam a importância da segurança da informação e exigem controles de acesso e gerenciamento de riscos.

Aspecto	ISO/IEC 27001	PCI DSS
Requisitos	Política de segurança, avaliação contínua de riscos, controles amplos de segurança	12 requisitos focados na proteção de dados de cartão de crédito
Setores de Atuação	TI, serviços financeiros, saúde e outros setores que lidam com informações sensíveis	Bancos, e-commerce, operadoras de pagamento, indústrias de transações financeiras
Benefícios	Segurança geral da informação, aumento de confiança no mercado, conformidade legal	Proteção de dados de pagamento, redução de fraudes, evitar multas
Gestão de Riscos	Abordagem ampla, focada em todos os riscos relacionados à informação	Focada exclusivamente em riscos de dados de pagamento