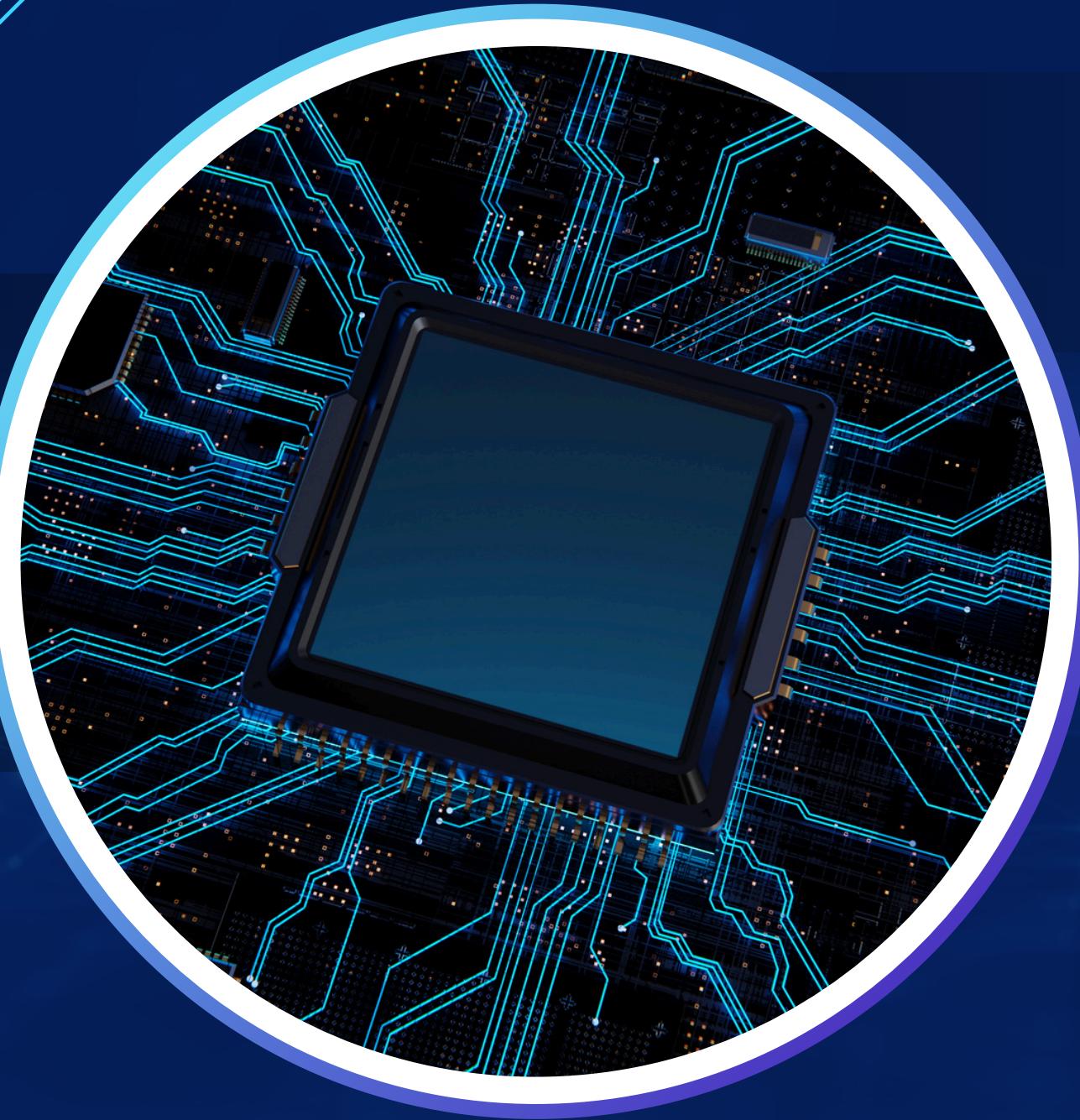


ISO/IEC 27001



E
PCI DSS

REQUISITOS PARA CERTIFICAÇÃO



ISO/IEC 27001:

- Requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o Sistema de Gestão de Segurança da Informação (SGSI).
- Envolve análise de riscos, controles e processos contínuos para garantir a segurança da informação.

PCI DSS:

- Requisitos específicos para proteger dados de cartões de pagamento.
- Foca na proteção dos dados durante transações e armazenamento, com requisitos claros de criptografia, controle de acesso e monitoramento.

■ ISO/IEC 27001:

- Utilizada por empresas de diversos setores, incluindo tecnologia, saúde, finanças e governo.
- Ideal para organizações que buscam garantir a segurança de toda a informação, independentemente do tipo de dado.

■ PCI DSS:

- Focada no setor de pagamento e transações financeiras.
- Usada por empresas que lidam com cartões de crédito, processadores de pagamento e outros envolvidos em transações financeiras.

SETORES DE ATUAÇÃO

BENEFÍCIOS DE OBTER CADA CERTIFICAÇÃO

■ ISO/IEC 27001:

- Protege dados sensíveis e melhora a confiança de clientes e parceiros.
- Atende a regulamentações de segurança e pode reduzir riscos relacionados a vazamentos de dados.



■ PCI DSS:

- Garantia de conformidade com as regulamentações de segurança de dados financeiros.
- Reduz o risco de fraudes e outros problemas relacionados ao uso indevido de cartões de pagamento.



DIFERENÇAS NA ABORDAGEM DE GESTÃO DE RISCOS

■ ISO/IEC 27001:

- Foca em uma abordagem de gestão de riscos mais ampla e contínua, que abrange todos os aspectos da segurança da informação dentro da organização.
- Exige a identificação, avaliação e mitigação de riscos em vários níveis da organização.

05

www.reallygreatsite.com



■ PCI DSS:

- Abordagem focada principalmente em mitigar riscos relacionados ao processamento, armazenamento e transmissão de dados de cartões de pagamento.
- Exige a implementação de medidas de segurança específicas, como criptografia e controles de acesso restritos.



ISO/IEC 27001 vs. PCI DSS

- ISO/IEC 27001

A ISO/IEC 27001 define os requisitos para implementar um Sistema de Gestão de Segurança da Informação (SGSI), focado na proteção de dados e na gestão de riscos. Ela é aplicável a qualquer organização e ajuda a criar uma estrutura robusta para proteger informações sensíveis, promover a melhoria contínua e garantir conformidade com regulamentos de segurança.

ISO/IEC 27001	PCI DSS
	
REQUISITOS PARA CERTIFICAÇÃO Requisitos para estabelecer e melhorar um SGSI	REQUISITOS PARA PROTEGER DADOS Requisitos para proteger dados de cartões de pagamento
SETORES DE ATUAÇÃO Empresas de diversos setores, incluindo tecnologia, saúde e governo	BENEFÍCIOS Conformidade com regulamentos de segurança de dados
BENEFÍCIOS Protege dados sensíveis, confiança de clientes e parceiros	DIFERENÇAS NA ABORDAGEM DE GESTÃO DE RISCOS Mitigação de riscos focada em dados de pagamento
DIFERENÇAS NA ABORDAGEM DE GESTÃO DE RISCOS	
Gestão de riscos abrangente e continua	Mitigação de riscos focada em dados

- PCI DSS (esquerda)

O PCI DSS estabelece requisitos para proteger os dados dos cartões de pagamento, aplicáveis a organizações que processam ou armazenam informações de cartões de crédito e débito. A certificação garante segurança no manuseio dos dados financeiros, com ênfase em criptografia, controle de acessos e auditorias regulares, aumentando a confiança dos consumidores e prevenindo fraudes.



OBRIGADO PELA
ATENÇÃO