Iago da rocha silva

Rm: 824139839

1. Requisitos para Certificação

• ISO/IEC 27001: Focado na implementação de um Sistema de Gestão da Segurança da Informação (SGSI). Requer uma política de segurança formal, avaliação de riscos, e controles em várias áreas (segurança física, gestão de ativos, controle de acessos, etc.).

• PCI DSS: Desenvolvido para proteger dados de cartões de crédito. Exige medidas de proteção em seis áreas principais, como redes seguras, controle de acessos e monitoramento regular de redes e sistemas.

2. Setores de Atuação

• ISO/IEC 27001: Aplicável em diversos setores, como finanças, saúde, tecnologia, telecomunicações e qualquer indústria que precise proteger dados sensíveis.

• PCI DSS: Exclusivamente voltado para empresas que processam, armazenam ou transmitem dados de cartões de pagamento, como e-commerces, bancos e varejistas.

3. Benefícios de Cada Certificação

• ISO/IEC 27001: Melhora a confiança com clientes e parceiros, oferece uma abordagem ampla para a segurança da informação e auxilia na conformidade com regulamentações.

• PCI DSS: Protege contra fraudes de pagamento, evita multas por descumprimento de normas financeiras e assegura clientes de que seus dados estão protegidos.

4. Diferenças na Abordagem de Gestão de Riscos

• ISO/IEC 27001: Tem uma abordagem mais ampla, focada em identificar, avaliar e mitigar riscos em todos os tipos de dados e processos de negócios.

• PCI DSS: É mais restrita, focando exclusivamente nos riscos relacionados aos dados de cartões de pagamento e operações associadas.

Infográfico:

Você pode criar um infográfico comparando os pontos acima com colunas ou diagramas para destacar as diferenças e similaridades, como:

1. Título: “Comparativo entre ISO/IEC 27001 e PCI DSS”

2. Comparações lado a lado para cada seção (Requisitos, Setores, Benefícios, Gestão de Riscos).

3. Use ícones para representar setores, certificações, e gestão de riscos, facilitando a visualização.