| **Critério** | **ISO/IEC 27001** | **PCI DSS** |
| --- | --- | --- |
| Abrangência | Qualquer empresa | Empresas que lidam com cartões |
| Tipo de Requisitos | Flexíveis, baseados em risco | Técnicos, normativos |
| Certificação | Voluntária | Obrigatória (para quem processa cartões) |
| Setores de atuação | Todos os setores | Bancos, e-commerce, varejo |
| Auditorias | Auditoria externa por certificadora | Auditoria QSA ou autoavaliação |
| Benefícios principais | Gestão completa de segurança, reputação | Evita fraudes e penalidades financeiras |
| Foco principal | Sistema de gestão de segurança da informação | Proteção de dados de pagamento |