# Certificações em Segurança da Informação

#### **Exercício 2 - Aula 6**

Davi Deosmar Batista Oliveira Miranda – RA: 823.212.282

Silas Rodrigues Nascimento – RA: 823.273.38

**Certificações em Segurança da Informação** – **Atividade**

|  |  |  |
| --- | --- | --- |
|  | ISO/IEC 27001 | PCI DSS |
| Requisitos para a certificação | Para obter a certificação ISO/IEC 27001, é preciso implementar um Sistema de Gerenciamento de Segurança da Informação (SGSI) que inclua requisitos como análise e tratamento de riscos, definição de políticas de segurança, compromisso da alta liderança e monitoramento contínuo do sistema. A empresa deve atender a todas as cláusulas da norma, como contexto da organização, liderança, planejamento, suporte, operação, avaliação de desempenho e melhoria. | Para obter a conformidade com o PCI DSS, é preciso atender a 12 requisitos principais, que incluem:   * Instalar e manter um firewall * Eliminar a configuração padrão do fornecedor * Proteger os dados armazenados do titular do cartão * Criptografar a transmissão de dados de pagamento * Atualizar regularmente o software antivírus * Implantar sistemas e aplicativos seguros * Restringir acesso aos dados do titular do cartão conforme necessário * Atribuir identificação de acesso do usuário * Restringir o acesso físico aos dados * Rastrear e monitorar o acesso à rede * Testar processos e sistemas continuamente em busca de vulnerabilidades * Criar e manter uma política de infosec |
| Setor de atuação | A norma ISO 27001 não se restringe a um único setor de atuação e é aplicável a qualquer organização, de qualquer tamanho e segmento, que precise proteger suas informações e estabelecer um Sistema de Gestão de Segurança da Informação (SGSI). Isso inclui desde grandes corporações até pequenas e médias empresas em áreas como saúde, finanças e tecnologia. | O PCI DSS (Payment Card Industry Data Security Standard) é um padrão de segurança de dados aplicado a todas as entidades envolvidas no processamento, armazenamento ou transmissão de dados de titulares de cartões. Isso significa que sua área de atuação não se restringe a um único setor, mas se aplica a qualquer negócio que lide com pagamentos de cartão de crédito |
| Benefícios da certificação | A certificação ISO 27001 oferece benefícios como aumento da confiança de clientes e parceiros, redução de riscos de segurança e custos com incidentes, conformidade com regulamentações (como a LGPD) e melhoria da gestão de informações. | Os benefícios do PCI DSS incluem proteção de dados do titular do cartão contra fraudes e acessos não autorizados, aumento da confiança do cliente e da credibilidade da empresa, e a prevenção de perdas financeiras e multas associadas a violações de dados. |
| Diferenças na abordagem | Essa certificação define os requisitos, processos e normas a serem seguidas para garantir uma gestão de segurança da informação eficaz. De modo geral, diversos especialistas da área se unem para unir seus conhecimentos e experiências para criar um padrão bem definido e seguro para todos. As ações definidas pela norma realizam a gestão de riscos e protegem os dados das empresas de forma eficiente e prática. | A estrutura do PCI DSS orienta as empresas com processos robustos para proteger os dados de transação do titular do cartão e as informações de [autenticação](https://www.cloudflare.com/learning/access-management/what-is-authentication/) do cartão.Destina-se a proteger os dados do titular do cartão e os dados de autenticação com requisitos que ajudam a prevenir, detectar e reagir a incidentes de segurança. |