Atividade 2

Comparativo de Certificações em Segurança da Informação

PCI e DSS

Requisitos para certificação e Benefícios de obter cada certificação

A **certificação PCI DSS (Payment Card Industry Data Security Standard)** é um conjunto de padrões de segurança criado para proteger as informações de cartões de pagamento e prevenir fraudes. Empresas que armazenam, processam ou transmitem dados de cartões de pagamento precisam cumprir os requisitos PCI DSS para garantir a segurança dessas informações.

O PCI DSS é mantido pelo **PCI Security Standards Council**, fundado por grandes marcas de cartões, como Visa, MasterCard, American Express, JCB e Discover. A certificação PCI DSS envolve o cumprimento de 12 requisitos principais, organizados em seis objetivos de controle de segurança.

Objetivos e Requisitos PCI DSS:

1. Construir e manter uma rede segura

- **Requisito 1: Instalar e manter uma configuração de firewall** para proteger os dados dos titulares de cartões.

    - Garantir que o firewall esteja configurado corretamente para impedir acessos não autorizados e proteger as redes que armazenam, processam ou transmitem dados de cartões de pagamento.
- **Requisito 2: Não usar senhas padrão do fabricante ou outras configurações de segurança padrão**.
    - Modificar todas as senhas e configurações padrão em dispositivos, sistemas operacionais, roteadores e firewalls, pois essas configurações são vulneráveis a ataques.

2. Proteger os dados dos titulares de cartões

- **Requisito 3: Proteger os dados armazenados dos titulares de cartões**.
    - Dados sensíveis, como números de cartão de crédito (PAN), devem ser criptografados e truncados, exceto quando estritamente necessário. Informações como CVV ou PIN não podem ser armazenadas após a autorização.
- **Requisito 4: Criptografar a transmissão dos dados dos titulares de cartões através de redes abertas e públicas**.
    - Sempre que os dados forem transmitidos por redes não seguras (como a internet), eles devem ser criptografados utilizando protocolos seguros como TLS, SSH ou IPsec.

3. Manter um programa de gerenciamento de vulnerabilidades

- **Requisito 5: Usar e atualizar regularmente programas antivírus ou soluções de segurança contra malware**.
    - Proteger todos os sistemas contra vírus, malware e outras ameaças, garantindo que essas soluções sejam regularmente atualizadas e configuradas corretamente.
- **Requisito 6: Desenvolver e manter sistemas e aplicativos seguros**.
    - Aplicar correções e patches de segurança de forma proativa para corrigir vulnerabilidades em sistemas operacionais, softwares e aplicativos que processam dados de cartões.

4. Implementar medidas rigorosas de controle de acesso

- **Requisito 7: Restringir o acesso aos dados dos titulares de cartões conforme a necessidade de negócios (privilégios mínimos)**.
    - O acesso aos dados de cartões deve ser concedido apenas a funcionários ou sistemas que realmente precisem deles para realizar suas funções.
- **Requisito 8: Atribuir um ID exclusivo a cada pessoa com acesso ao sistema**.
    - Para rastrear atividades e prevenir o uso compartilhado de contas, cada usuário que acessar sistemas de processamento de cartões deve ter um

ID único. Isso permite auditorias e rastreamento de responsabilidades.

- **Requisito 9: Restringir o acesso físico aos dados dos titulares de cartões**.
    - Garantir que locais físicos que armazenam informações de cartões estejam protegidos contra acesso não autorizado (servidores, estações de trabalho, arquivos físicos, etc.).

5. Monitorar e testar regularmente as redes

- **Requisito 10: Rastrear e monitorar todos os acessos aos recursos de rede e aos dados dos titulares de cartões**.
    - Implementar mecanismos de monitoramento e geração de logs que rastreiem todos os acessos e atividades nos sistemas que processam dados de cartões. Os logs devem ser revisados regularmente para detectar atividades suspeitas.
- **Requisito 11: Testar regularmente os sistemas e processos de segurança**.
    - Realizar testes de penetração e avaliações de vulnerabilidades periodicamente, além de monitorar redes e sistemas para detectar possíveis intrusões ou falhas.

6. Manter uma política de segurança da informação

- **Requisito 12: Manter uma política que aborda a segurança da informação para todos os funcionários**.
    - Implementar uma política de segurança abrangente que cubra a proteção dos dados dos cartões e defina as responsabilidades de todos os funcionários. Isso inclui treinamento regular, orientações claras e processos documentados.

Níveis de Conformidade PCI DSS:

As exigências para certificação PCI DSS variam de acordo com o volume de transações da organização, dividido em quatro níveis:

- **Nível 1**: Empresas que processam mais de 6 milhões de transações anuais. Requerem uma auditoria anual realizada por um auditor qualificado (QSA - Qualified Security Assessor) e testes trimestrais de vulnerabilidade por um provedor de varredura aprovado (ASV - Approved Scanning Vendor).
- **Nível 2**: Empresas que processam entre 1 milhão e 6 milhões de transações anuais. Precisam preencher um Questionário de Autoavaliação (SAQ - Self-Assessment Questionnaire) e realizar testes trimestrais de vulnerabilidade por um ASV.
- **Nível 3**: Empresas que processam entre 20.000 e 1 milhão de transações e-commerce por ano. Exigem a

submissão do SAQ e testes trimestrais de vulnerabilidade.

- **Nível 4**: Empresas que processam menos de 20.000 transações e-commerce ou até 1 milhão de transações presenciais anuais. Requerem o SAQ e testes trimestrais de vulnerabilidade, mas com menos rigor que os níveis superiores.

Benefícios da Certificação PCI DSS:

- **Proteção contra fraudes**: A implementação dos controles recomendados pelo PCI DSS ajuda a mitigar os riscos de fraudes envolvendo cartões de crédito.
- **Conformidade legal**: Muitas jurisdições exigem que empresas que processam dados de cartões estejam em conformidade com o PCI DSS para evitar sanções.
- **Reputação e confiança**: Estar em conformidade com o PCI DSS aumenta a confiança dos clientes e parceiros de negócios, já que demonstra compromisso com a segurança dos dados.

Conclusão:

A obtenção da certificação PCI DSS exige o cumprimento de todos os 12 requisitos e depende da estrutura de segurança e das práticas da empresa. A conformidade é um processo contínuo, exigindo monitoramento e atualizações constantes para garantir a proteção contínua contra ameaças e manter a confiança nas transações financeiras.

Setores de atuação

1. Varejo (Físico e E-commerce)

- **Setor de Varejo Físico**: Lojas de varejo, supermercados, postos de gasolina e quaisquer outros estabelecimentos que aceitem pagamentos com cartão em pontos de venda físicos precisam seguir as normas PCI DSS. Isso inclui a proteção dos dados de cartão capturados em terminais de ponto de venda (POS).
- **E-commerce**: Lojas online e outros serviços que aceitam pagamentos via internet são especialmente vulneráveis a ataques cibernéticos, como roubo de dados e fraude. O PCI DSS é crucial para proteger os dados dos clientes em transações online e garantir a segurança durante o armazenamento e transmissão das informações.

2. Bancos e Instituições Financeiras

- **Bancos**: Instituições financeiras, como bancos e cooperativas de crédito, que processam pagamentos com cartão precisam aderir ao PCI DSS. Eles lidam com grandes volumes de transações diárias e precisam proteger informações de cartão e de contas bancárias.
- **Processadoras de Pagamento (Payment Processors)**: Empresas que oferecem serviços de processamento de

pagamentos com cartão de crédito e débito, como adquirentes e gateways de pagamento, são diretamente responsáveis por garantir a conformidade com PCI DSS.

- **Instituições de Crédito e Fintechs**: Empresas que oferecem serviços de crédito, empréstimos ou gestão de finanças digitais (como fintechs) precisam proteger as informações financeiras dos clientes, tornando a certificação PCI DSS um requisito essencial para essas operações.

3. Setor Hoteleiro e de Viagens

- **Hotéis e Resorts**: O setor de hospitalidade lida com grandes volumes de transações com cartão, desde reservas online até pagamentos presenciais nas instalações. Isso inclui pagamentos em restaurantes, spas e outros serviços oferecidos no local. Garantir a conformidade com PCI DSS é crucial para evitar a exposição de dados dos hóspedes.
- **Companhias Aéreas e Agências de Viagem**: As companhias aéreas e as agências de viagens, que processam pagamentos de bilhetes e reservas de hotéis, também precisam garantir que seus sistemas estejam em conformidade com o PCI DSS para proteger os dados dos passageiros.

4. Saúde

- **Hospitais e Clínicas**: Instituições de saúde que aceitam pagamentos com cartão, tanto para consultas quanto para procedimentos, precisam seguir as normas PCI DSS para garantir a proteção dos dados dos pacientes durante o pagamento.
- **Farmácias**: Assim como em outras áreas da saúde, farmácias que processam pagamentos com cartão também devem estar em conformidade com PCI DSS para proteger as transações de seus clientes.

5. Educação

- **Instituições de Ensino**: Universidades, faculdades e escolas que aceitam pagamentos de mensalidades, taxas de inscrição ou doações com cartão de crédito precisam garantir a segurança dessas transações. Isso inclui pagamentos online, realizados por meio de portais de estudantes ou doadores.

6. Telecomunicações

- **Provedores de Serviços de Telecomunicações**: Operadoras de telefonia, internet e TV a cabo que aceitam pagamentos com cartão de crédito ou débito em contas recorrentes precisam seguir as normas do PCI DSS para garantir a proteção dos dados dos clientes.

7. Setor de Entretenimento

- **Parques Temáticos e Eventos**: Empresas de entretenimento que vendem ingressos para shows, concertos, parques temáticos e eventos esportivos muitas vezes aceitam pagamentos com cartão, tanto online quanto presencialmente, e, portanto, devem cumprir os requisitos PCI DSS.
- **Cassinos e Loterias**: Esses estabelecimentos lidam com grandes volumes de transações financeiras diárias e são obrigados a proteger os dados de seus clientes, sendo obrigatória a adesão às normas PCI DSS.

8. Setor de Alimentação

- **Restaurantes e Cadeias de Fast Food**: Restaurantes e franquias de alimentos que aceitam pagamentos com cartão de crédito ou débito precisam seguir as normas PCI DSS. Isso se aplica tanto a transações presenciais quanto a pedidos online ou por meio de aplicativos de entrega.

9. Transportes

- **Companhias de Transporte e Logística**: Empresas de transporte público, táxis e serviços de entrega que aceitam pagamentos com cartão precisam garantir a conformidade com PCI DSS para proteger as informações de pagamento de seus clientes.

10. Organizações Sem Fins Lucrativos

- **ONGs e Fundações**: Muitas organizações sem fins lucrativos aceitam doações por meio de cartões de crédito ou débito, tanto online quanto em eventos beneficentes. Para garantir a segurança dos dados dos doadores, essas organizações devem aderir ao PCI DSS.

11. Serviços de Assinatura

- **Plataformas de Streaming e Serviços de Assinatura Online**: Empresas que operam com modelos de pagamento recorrente, como plataformas de streaming, serviços de software como serviço (SaaS) e outros tipos de assinatura, precisam garantir que suas transações de pagamento estejam em conformidade com as normas PCI DSS.

12. Provedores de Serviços de TI e Nuvem

- **Provedores de Infraestrutura de TI e Serviços na Nuvem**: Empresas que fornecem infraestrutura como serviço (IaaS), plataformas como serviço (PaaS) e software como serviço (SaaS), especialmente aquelas que hospedam ou gerenciam sistemas de pagamento para outras organizações, precisam estar em conformidade com o PCI DSS, garantindo a segurança dos dados de seus clientes e das transações que hospedam.

Conclusão:

O PCI DSS é essencial para qualquer setor que processe, armazene ou transmita dados de cartões de pagamento. A conformidade com essas normas é crucial para garantir a segurança das transações e proteger a privacidade dos clientes, reduzindo o risco de fraudes e violações de dados.

Diferenças na abordagem de gestão de riscos

As abordagens de gestão de riscos entre PCI (Payment Card Industry) e DSS (Data Security Standard) diferem principalmente em seus focos, escopos e métodos de implementação. Aqui estão as principais diferenças na abordagem de gestão de riscos entre PCI e DSS:

1. Foco e Escopo

- **PCI DSS**:
    - **Foco**: O PCI DSS é especificamente projetado para proteger os dados dos titulares de cartões e garantir a segurança das transações de pagamento. Seu foco é a proteção das informações de pagamento, como números de cartão de crédito, dados pessoais e informações sensíveis.
    - **Escopo**: O escopo é limitado a organizações que processam, armazenam ou transmitem dados de

cartões de pagamento, abrangendo um conjunto específico de requisitos de segurança que devem ser atendidos para garantir a conformidade.

- **DSS (como outros padrões de segurança de dados)**:
  - **Foco**: O DSS pode se referir a vários padrões de segurança de dados (como ISO/IEC 27001), que têm uma abordagem mais abrangente em relação à segurança da informação. A gestão de riscos aqui se aplica a uma gama mais ampla de dados, sistemas e processos de negócios.
  - **Escopo**: O escopo de um DSS é mais amplo e pode incluir a proteção de todos os tipos de dados (não apenas dados de pagamento) em uma organização, abrangendo políticas, procedimentos e controles de segurança mais gerais.

2. Metodologia de Gestão de Riscos

- **PCI DSS**:
  - **Abordagem Prescritiva**: O PCI DSS oferece uma lista específica de requisitos que as organizações devem seguir, como a instalação de firewalls, a criptografia de dados e a realização de testes de segurança. A abordagem é mais prescritiva, fornecendo diretrizes claras sobre como mitigar riscos específicos relacionados a dados de pagamento.

    - **Foco na Conformidade**: A ênfase está na conformidade com os requisitos do padrão. As organizações devem realizar auditorias e avaliações regulares para garantir que estejam seguindo todas as diretrizes do PCI DSS.
- **DSS (como outros padrões de segurança de dados)**:
    - **Abordagem Baseada em Risco**: Muitas normas DSS, como a ISO 27001, utilizam uma abordagem baseada em risco. As organizações são encorajadas a identificar e avaliar riscos específicos para sua operação e implementar controles de segurança adequados com base em uma análise de risco mais abrangente.
    - **Flexibilidade e Adaptação**: A abordagem é mais flexível, permitindo que as organizações adaptem suas práticas de gestão de riscos com base em seu contexto, objetivos de negócios e requisitos legais específicos. Isso permite uma personalização que pode ser mais eficaz em lidar com riscos específicos.

3. Processo de Avaliação de Risco

- **PCI DSS**:
    - **Avaliação Direcionada**: O processo de avaliação de risco no contexto do PCI DSS é frequentemente focado em vulnerabilidades relacionadas a dados de pagamento e no cumprimento dos requisitos do

padrão. As avaliações são feitas em relação a requisitos específicos e padrões estabelecidos pelo PCI.

    - **Relatórios e Certificações**: Organizações que não atendem aos requisitos do PCI DSS podem enfrentar penalidades financeiras e riscos de reputação. Portanto, a gestão de riscos é muitas vezes orientada para garantir a conformidade e evitar consequências legais.
- **DSS (como outros padrões de segurança de dados)**:
    - **Avaliação Abrangente**: O processo de avaliação de risco em um DSS é mais abrangente e pode incluir a identificação de ameaças e vulnerabilidades em toda a organização, independentemente de serem relacionadas a dados de pagamento ou não. Isso envolve uma análise holística de riscos e a avaliação de controles de segurança em diferentes áreas.
    - **Foco na Melhoria Contínua**: Muitas normas DSS promovem a melhoria contínua dos processos de segurança da informação, incentivando a revisão e atualização regulares das políticas e práticas de gestão de riscos.

4. Documentação e Relatórios

- **PCI DSS**:

    - **Documentação Específica**: O PCI DSS exige documentação específica sobre os controles implementados, como a manutenção de logs de auditoria, registros de testes de segurança e relatórios de conformidade.
    - **Relatório de Conformidade**: As organizações precisam fornecer relatórios de conformidade anuais (por meio de um auditor qualificado) ou relatórios de autoavaliação, dependendo do nível de conformidade.
- **DSS (como outros padrões de segurança de dados)**:
    - **Documentação Abrangente**: Embora também exija documentação, as normas DSS podem ser menos prescritivas em termos de relatórios específicos. A documentação pode abranger uma ampla gama de políticas, procedimentos e práticas de segurança, dependendo do escopo e das necessidades da organização.
    - **Avaliação Contínua**: As organizações são incentivadas a manter registros contínuos de suas práticas de gestão de riscos e a realizar avaliações regulares para garantir que os controles permaneçam eficazes e relevantes.

Conclusão

Em resumo, a abordagem de gestão de riscos do PCI DSS é focada, prescritiva e voltada para a conformidade com

padrões específicos de proteção de dados de pagamento. Por outro lado, outras abordagens de DSS podem ser mais amplas, flexíveis e orientadas para a identificação e mitigação de uma gama mais ampla de riscos à segurança da informação. Ambas as abordagens são importantes, mas a escolha entre elas deve ser baseada nas necessidades específicas da organização e no contexto em que opera.