Payment Card Industry
Padrão de Segurança de Dados

Questionário de Autoavaliação D para Comerciantes e Atestado de Conformidade

Para uso com o PCI DSS Versão 4.0.1

Data de Publicação: Outubro de 2024

TERMO DE RECONHECIMENTO: A versão em inglês deste documento, conforme disponibilizada no site do PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês, a versão em inglês disponibilizada no local mencionado prevalecerá.

Alterações no Documento

Data	Versão do PCI DSS	Revisão do SAQ	Descrição
Outubro de 2008	1.2		Para alinhar o conteúdo com o novo PCI DSS v1.2 e implementar pequenas mudanças observadas desde a v1.1 original.
Outubro de 2010	2.0		Para alinhar o conteúdo com os novos requisitos e procedimentos de teste do PCI DSS v2.0.
Fevereiro de 2014	3.0		Para alinhar o conteúdo com os requisitos e procedimentos de teste do PCI DSS v3.0 e incorporar opções de resposta adicionais.
Abril de 2015	3.1		Atualizado para alinhar com o PCI DSS v3.1. Para obter detalhes sobre as mudanças do PCI DSS, consulte o PCI DSS – Resumo das Alterações do PCI DSS da versão 3.0 para 3.1.
Julho de 2015	3.1	1.1	Atualizado para remover referências a “práticas recomendadas” antes de 30 de junho de 2015 e remover a opção de relatório do PCI DSS v2 para o Requisito 11.3.
Abril de 2016	3.2	1.0	Atualizado para alinhar com o PCI DSS v3.2. Para obter detalhes sobre as mudanças do PCI DSS, consulte o PCI DSS – Resumo das Alterações do PCI DSS da versão 3.1 para 3.2.
Janeiro de 2017	3.2	1.1	Numeração de versão atualizada para alinhar com outros SAQs.
Junho de 2018	3.2.1	1.0	Atualizado para alinhar com o PCI DSS v3.2.1. Para obter detalhes sobre as mudanças do PCI DSS, consulte o PCI DSS – Resumo das Alterações do PCI DSS da versão 3.2 para 3.2.1.
Abril de 2022	4.0		Atualizado para alinhar com o PCI DSS v4.0. Para obter detalhes sobre as mudanças do PCI DSS, consulte o PCI DSS – Resumo das Alterações do PCI DSS da versão 3.2.1 para 4.0. Informações reorganizadas, renomeadas e expandidas na seção “Preenchendo o Questionário de Autoavaliação” (anteriormente intitulada “Antes de Começar”). Conteúdo alinhado nas Seções 1 e 3 do Atestado de Conformidade (AOC) com o Relatório PCI DSS v4.0 sobre AOC de Conformidade. Adicionados apêndices para dar suporte a novas respostas de relatórios.
Dezembro de 2022	4.0	1	Removido “Implementado com Correções” como uma opção de relatório da tabela Respostas aos Requisitos, Atestado de Conformidade (AOC) Parte 2g, coluna de Resposta do SAQ Seção 2, e AOC Seção 3. Removido também o antigo Apêndice C. Adicionado “Implementado com CCW” ao AOC Seção 3. Adicionado as orientações para responder aos requisitos com datas futuras. Adicionados esclarecimentos secundários e apresentados erros de digitação.

Outubro de 2024	4.0.1		Atualizado para alinhamento com o PCI DSS v4.0.1. Para obter detalhes sobre as mudanças do PCI DSS, consulte o PCI DSS – *Resumo das Alterações do PCI DSS da versão 4.0 para 4.0.1.* Adicionado o Guia de Recursos ASV à seção "Recursos Adicionais do PCI SSC."

Índice

Preenchendo o Questionário de Autoavaliação

Critérios de Elegibilidade do Comerciante para o Questionário D de Autoavaliação

Os Questionário de Autoavaliação (SAQ) D para Comerciantes se aplica a comerciantes qualificados para preencher um questionário de autoavaliação, mas que não atendem aos critérios de nenhum outro tipo de SAQ. Exemplos de ambientes comerciais aos quais o SAQ D pode se aplicar incluem, mas não se limitam a:

- Comerciantes de comércio eletrônico que aceitam dados da conta em seu site.
- Comerciantes com armazenamento eletrônico de dados da conta.
- Comerciantes que não armazenam eletronicamente os dados da conta, mas que não atendem aos critérios de outro tipo de SAQ.
- Comerciantes com ambientes que podem atender aos critérios de outro tipo de SAQ, mas que possuem requisitos adicionais do PCI DSS aplicáveis ao seu ambiente.

Este SAQ não é aplicável para prestadores de serviço.

Definindo os Dados da Conta, Dados do Titular do Cartão e Dados Confidenciais de Autenticação

O PCI DSS destina-se a todas as entidades que armazenam, processam ou transmitem dados do titular do cartão (CHD) e/ou dados de autenticação confidenciais (SAD) ou podem impactar na segurança dos dados do titular do cartão e/ou dados de autenticação confidenciais . Os dados do titular do cartão e os dados de autenticação confidenciais são considerados dados da conta e são definidos da seguinte forma:

Dados da Conta	
Os Dados do Titular do Cartão incluem:	**Os Dados de Autenticação Confidenciais incluem:**
• Número da Conta Principal (PAN) • Nome do Titular do Cartão • Data de Validade • Código do Serviço	• Dados de rastreamento completo (dados de tarja magnética ou equivalente em um chip) • Código de verificação do cartão • Bloqueios de PINs/PIN

Consulte a Seção 2 do PCI DSS, *Informações de Aplicabilidade do PCI DSS*, para obter mais detalhes.

Etapas de Conclusão da Autoavaliação do PCI DSS

1. Confirme analisando os critérios de elegibilidade neste SAQ e no documento de *Instruções e Diretrizes do Questionário de Autoavaliação* no site do PCI SSC se este é o SAQ correto para o ambiente do comerciante.
2. Confirme se o ambiente do comerciante está no escopo adequado.
3. Avalie o ambiente quanto à conformidade com os requisitos do PCI DSS.
4. Preencha todas as seções deste documento:
   - Seção 1: Informações de Avaliação (Partes 1 e 2 do Atestado de Conformidade (AOC) – Informações de Contato e Resumo Executivo).
   - Seção 2: Questionário de Autoavaliação D para Comerciantes.
   - Seção 3: Detalhes da Validação e Atestado (Partes 3 e 4 do AOC – Plano de Ação e Validação do PCI DSS para Requisitos Não Conformes (se a Parte 4 for aplicável)).
5. Envie o SAQ e o AOC, juntamente com qualquer outra documentação solicitada - como relatórios de varreduras ASV - para a organização solicitante (as organizações que gerenciam programas de conformidade, como bandeiras de pagamento e adquirentes).

Teste Esperado

As instruções fornecidas na coluna "Teste Esperado" são baseadas nos procedimentos de teste no PCI DSS e fornecem uma descrição de alto nível dos tipos de atividades de teste que um comerciante deve realizar para verificar se um requisito foi atendido.

A intenção por trás de cada método de teste é descrita a seguir:

Examine: O comerciante avalia criticamente a evidência de dados. Os exemplos comuns incluem documentos (eletrônicos ou físicos), capturas de tela, arquivos de configuração, registros de auditoria e arquivos de dados.

Observe: O comerciante observa uma ação ou vê algo no ambiente. Exemplos de objetos de observação incluem pessoal executando tarefas ou processos, software ou componentes do sistema executando uma função ou respondendo a entrada, configurações/definições do sistema, condições ambientais e controles físicos.

Entreviste: O comerciante conversa com o pessoal individualmente. Os objetivos da entrevista podem incluir a confirmação se uma atividade é realizada, descrições de como uma atividade é realizada e se o pessoal tem conhecimento ou compreensão particular.

Os métodos de teste destinam-se a permitir que o comerciante demonstre como atendeu a um requisito. Os itens específicos a serem examinados ou observados e o pessoal a ser entrevistado devem ser adequados tanto para o requisito que está sendo avaliado quanto para a implementação particular do comerciante.

Detalhes completos dos procedimentos de teste para cada requisito podem ser encontrados no PCI DSS.

Respostas do Requisito

Para cada item de requisito, há opções de respostas para indicar o status do comerciante em relação a esse requisito. ***Apenas uma resposta deve ser selecionada para cada item de requisito.***

Uma descrição do significado de cada resposta é fornecida na tabela abaixo:

Resposta	Quando usar esta resposta:
Implementado	O teste esperado foi realizado e todos os elementos do requisito foram atendidos conforme declarado.
Implementado com CCW (Planilha de Controles de Compensação)	O teste esperado foi realizado e o requisito foi atendido com a ajuda de um controle de compensação. Todas as respostas nesta coluna exigem o preenchimento de uma Planilha de Controles de Compensação (CCW) no Apêndice B deste SAQ. Informações sobre o uso de controles de compensação e orientações sobre como preencher a planilha são fornecidas nos Apêndices B e C do PCI DSS.
Não Aplicável	O requisito não se aplica ao ambiente do comerciante. (Consulte “Diretrizes para Requisitos Não Aplicáveis” abaixo para obter exemplos.) Todas as respostas nesta coluna requerem uma explicação de apoio no Apêndice C deste SAQ.
Não Testado	O requisito não foi incluído para consideração na avaliação e não foi testado de forma alguma. (Consulte “Entendendo a Diferença entre Não Aplicável e Não Testado” abaixo para obter exemplos de quando esta opção deve ser usada). Todas as respostas nesta coluna requerem uma explicação de apoio no Apêndice D deste SAQ.
Não Implementado	Alguns ou todos os elementos do requisito não foram atendidos, ou estão em processo de implementação, ou exigem mais testes antes que o comerciante possa confirmar que estão implementados. As respostas nesta coluna podem exigir o preenchimento da Parte 4, se solicitado pela entidade à qual este SAQ será submetido. Essa resposta também é usada se um requisito não puder ser atendido devido a uma restrição jurídica. (Consulte “Exceção Jurídica” abaixo para obter mais orientações).

Diretrizes para Requisitos Não Aplicáveis

Embora muitos comerciantes que concluem o SAQ D precisem validar a conformidade com todos os requisitos do PCI DSS, algumas entidades com modelos de negócios muito específicos podem achar que alguns requisitos não se aplicam. Por exemplo, as entidades que não usam a tecnologia wireless em qualquer capacidade não devem cumprir os requisitos do PCI DSS que são específicos para o gerenciamento da tecnologia wireless. Da mesma forma, as entidades que não armazenam dados de contas eletronicamente a qualquer momento não devem cumprir os requisitos do PCI DSS relacionados ao armazenamento seguro de dados de contas (por exemplo, Requisito 3.5.1). Outro exemplo são os requisitos específicos para desenvolvimento de aplicativos e codificação segura (por exemplo, Requisitos 6.2.1 a 6.2.4), que se aplicam apenas a uma entidade com software sob medida (desenvolvido para a entidade por um terceiro de acordo com as suas especificações) ou software (desenvolvido pela entidade para uso próprio).

Para cada resposta em que Não Aplicável for selecionado neste SAQ, preencha o Apêndice C: Explicação dos Requisitos Observados como Não Aplicáveis.

Entendendo a Diferença entre Não Aplicável e Não Testado

Os requisitos considerados não aplicáveis a um ambiente devem ser verificados como tal. Usando o exemplo wireless acima, para um comerciante selecionar "Não Aplicável" para os Requisitos 1.3.3, 2.3.1, 2.3.2 e 4.2.1.2, o comerciante precisa primeiro confirmar que não há tecnologias wireless usadas no ambiente de dados do titular do cartão (CDE) ou que se conectam ao seu CDE. Uma vez confirmado, o comerciante pode selecionar “Não Aplicável” para esses requisitos específicos.

Se um requisito for completamente excluído da revisão sem qualquer consideração quanto à sua *possível* aplicação, a opção “Não Testado” deve ser selecionada. Exemplos de situações em que isso pode ocorrer podem incluir:

- Um comerciante é solicitado por seu adquirente a validar um subconjunto de requisitos, por exemplo, usando a Abordagem Priorizada do PCI DSS para validar apenas determinados marcos.
- Um comerciante está confirmando um novo controle de segurança que afeta apenas um subconjunto de requisitos, por exemplo, a implementação de uma nova metodologia de criptografia que requer apenas a avaliação dos Requisitos 2, 3 e 4 do PCI DSS.

Nesses cenários, a avaliação do comerciante inclui apenas determinados Requisitos do PCI DSS, embora outros requisitos também possam se aplicar ao seu ambiente.

Se algum requisito for completamente excluído da autoavaliação do comerciante, selecione Não Testado para esse requisito específico e preencha o Apêndice D: Explicação dos Requisitos Não Testados para cada entrada “Não Testado”. Uma avaliação com qualquer resposta Não Testado é uma avaliação “Parcial” do PCI DSS e será notada como tal pelo comerciante no Atestado de Conformidade na Seção 3, Parte 3 deste SAQ.

Diretrizes para Responder a Requisitos com Datas Futuras

Na Seção 2 abaixo, cada requisito ou item do PCI DSS com um período de implementação estendido inclui a seguinte observação*: "Este requisito [ou item] é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deverá ser totalmente considerado durante uma avaliação do PCI DSS."*

Esses novos requisitos não precisam ser incluídos em uma avaliação do PCI DSS até que a data futura tenha passado. Antes da referida data futura, quaisquer requisitos com uma data de implementação estendida que não tenham sido implementados pelo comerciante podem ser marcados como Não Aplicáveis e documentados no *Apêndice C: Explicação dos Requisitos Observados como Não Aplicáveis.*

Exceção Jurídica

Se sua organização estiver sujeita a uma restrição jurídica que a impeça de atender a um requisito do PCI DSS, selecione Não Implementado para esse requisito e preencha o atestado relevante na Seção 3, Parte 3 deste SAQ.

Observação: *Uma exceção jurídica é uma restrição legal devido a uma lei, regulamento ou requisito regulatório local ou regional, onde o cumprimento de um requisito do PCI DSS violaria essa lei, regulamento ou requisito regulatório.*

Obrigações contratuais ou aconselhamento jurídico não são restrições jurídicas.

Uso da Abordagem Personalizada

Os SAQs não podem ser usados para documentar o uso da Abordagem Personalizada para atender aos requisitos do PCI DSS. Por esse motivo, os Objetivos da Abordagem Personalizada não estão incluídos nos SAQs. As entidades que desejam validar usando a abordagem personalizada podem usar o Modelo de Relatório de Conformidade (ROC) do PCI DSS para documentar os resultados de sua avaliação.

O uso da Abordagem Personalizada não é suportado nos SAQs.

O uso da abordagem personalizada pode ser regulamentado por organizações que gerenciam programas de conformidade, como bandeiras de pagamento e adquirentes. Dúvidas sobre o uso de uma abordagem personalizada devem sempre ser encaminhadas a essas organizações. Isso inclui se uma entidade que é elegível para um SAQ pode, em vez disso, concluir um ROC para usar uma abordagem personalizada e se uma entidade é obrigada a usar um QSA ou pode usar um ISA para concluir uma avaliação usando a abordagem personalizada. Informações sobre o uso da Abordagem Personalizada podem ser encontradas nos Apêndices D e E do PCI DSS.

Recursos Adicionais do PCI SSC

Recursos adicionais que fornecem orientação sobre os requisitos do PCI DSS e como preencher o questionário de autoavaliação foram fornecidos abaixo para auxiliar no processo de avaliação.

Recurso	Inclui:
Requisitos e Procedimentos de Teste do Padrão de Segurança de Dados do PCI (PCI DSS)	▪ Diretrizes sobre o Escopo ▪ Diretrizes sobre a intenção de todos os requisitos do PCI DSS ▪ Detalhes dos procedimentos de teste ▪ Diretrizes sobre Controles de Compensação ▪ Apêndice G: Glossário de Termos, Abreviaturas e Acrônimos
Instruções e Diretrizes do SAQ	▪ Informações sobre todos os SAQs e seus critérios de elegibilidade ▪ Como determinar qual SAQ é o certo para sua organização
Perguntas Feitas com Frequência (FAQs)	▪ Diretrizes e informações sobre SAQs.
Glossário do PCI DSS On-line	▪ Termos, Abreviações e Acrônimos do PCI DSS
Complementos de Informações e Diretrizes	▪ Orientação sobre uma variedade de tópicos do PCI DSS, incluindo: – *Entendendo o Escopo do PCI DSS e a Segmentação de Rede* – *Garantia de Segurança de Terceiros* – *Orientação de Autenticação Multifator* – *Práticas Recomendadas para Manter a Conformidade com o PCI DSS*
Introdução ao PCI	▪ Recursos para comerciantes menores, incluindo: – *Guia para Pagamentos Seguros* – *Sistemas de Pagamentos Comuns* – *Perguntas para Fazer aos Seus Fornecedores* – *Glossário de Pagamento e Termos de Segurança da Informação* – *Noções Básicas de Firewall do PCI* – *Guia de Recursos ASV*

Esses e outros recursos podem ser encontrados no site do PCI SSC *(www.pcisecuritystandards.org)*.

As organizações são incentivadas a revisar o PCI DSS e outros documentos de suporte antes de iniciar uma avaliação.

Seção 1: Informações da Avaliação

Instruções para Submissão

Este documento deve ser preenchido como uma declaração dos resultados da autoavaliação do comerciante em relação aos *Requisitos e Procedimentos de Teste do Padrão de Segurança de Dados do Setor de Cartões de Pagamento [Payment Card Industry] (PCI DSS).* Preencha todas as seções. O comerciante é responsável por garantir que cada seção seja preenchida pelas partes relevantes, conforme aplicável. Entre em contato com a(s) entidade(s) para a(s) qual(ais) o Atestado de Conformidade (AOC) será enviado para procedimentos de relatório e envio.

Parte 1. Informações de Contato

Part 1a. Comerciante Avaliado

Nome da empresa:	
DBA (fazendo negócios como):	
Endereço para correspondência da empresa:	
Principal website da empresa:	
Nome de contato da empresa:	
Cargo de contato da empresa:	
Número de telefone do contato:	
Endereço de e-mail do contato:	

Parte 1b. Assessor

Forneça as informações a seguir para todos os assessores envolvidos na avaliação. Caso não haja um assessor para um determinado tipo de assessor, insira Não Aplicável.

Assessor(es) de Segurança Interna do PCI SSC	
Nome(s) do(s) ISA(s):	
Assessor de Segurança Qualificado	
Nome da empresa:	
Endereço para correspondência da empresa:	
Website da empresa:	
Nome do Assessor líder:	
Número de telefone do assessor:	
Endereço de e-mail do assessor:	
Número do certificado do assessor:	

Parte 2. Resumo Executivo

Parte 2a. Canais de Pagamento de Negócio do Comerciante (selecione todos os que se aplicam):

Indique todos os canais de pagamento usados pela empresa que estão incluídos nesta avaliação.

☐ Pedido por correspondência/pedido por telefone (MOTO, em inglês)

☐ Comércio eletrônico

☐ Cartão-presente

Algum canal de pagamento não está incluído nesta avaliação? Se sim, indique qual(ais) canal(is) não está(ão) incluído(s) na Avaliação e forneça uma breve explicação sobre por que o(s) canal(ais) foi(foram) excluído(s).	☐ Sim ☐ Não

Observação: *Caso o lojista possua um canal de pagamento não contemplado por este SAQ, consulte a(s) entidade(s) à(s) qual(ais) este AOC será submetido sobre a validação para os demais canais.*

Parte 2b. Descrição da Função com Cartões de Pagamento

Para cada canal de pagamento incluído nesta avaliação, tal como selecionado na Parte 2a acima, descreva como a empresa armazena, processa e/ou transmite os dados da conta.

Canal	Como a Empresa Armazena, Processa e/ou Transmite os Dados da Conta

Parte 2c. Descrição do Ambiente do Cartão de Pagamento

Forneça uma descrição de ***alto nível*** do ambiente coberto por esta avaliação. *Por exemplo:* • *Conexões dentro e fora do ambiente de dados do titular do cartão (CDE, em inglês).* • *Componentes críticos do sistema dentro do CDE, como dispositivos POI, bancos de dados, servidores web, etc., e quaisquer outros componentes de pagamento necessários, conforme aplicável.* • *Componentes do sistema que podem afetar a segurança dos dados da conta.*	
Indique se o ambiente inclui segmentação para reduzir o escopo da avaliação. *(Consulte a seção "Segmentação" do PCI DSS para obter orientação sobre segmentação.)*	☐ Sim ☐ Não

Parte 2. Resumo Executivo *(continuação)*

Parte 2d. Locais/Instalações Dentro do Escopo

Liste todos os tipos de locais/instalações físicas (por exemplo, locais de varejo, escritórios corporativos, data centers, call centers e salas de correspondência) no escopo da avaliação do PCI DSS.

Tipo de Instalação	Número Total de Localizações (Quantos locais deste tipo estão no escopo)	Local(ais) da Instalação (cidade, país)
Exemplo: Centros de dados	*3*	*Boston, MA, EUA*

Parte 2e. Produtos e Soluções Validados pelo PCI SSC

O comerciante usa algum item identificado em alguma Lista de Produtos e Soluções Validados do PCI SSC♦?

☐ Sim ☐ Não

Forneça as seguintes informações sobre cada item que o comerciante usa nas Listas de Produtos e Soluções Validados do PCI SSC.

Nome do Produto ou Solução Validado pelo PCI SSC	Versão do Produto ou Solução	Padrão do PCI SSC para o qual o Produto ou Solução foi Validado	Número de Referência na Lista do PCI SSC	Data de Validade da Lista (DD-MM-AAAA)
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA

♦ Para os propósitos deste documento, "Listas de Produtos e Soluções Validados" significa as listas de produtos, soluções e/ou componentes validados, que aparecem no site do PCI SSC (www.pcisecuritystandards.org) (por exemplo, Kits de Desenvolvimento de Software 3DS, Dispositivos PTS Aprovados, Software de Pagamento Validado, soluções de Criptografia Ponto a Ponto (P2PE), soluções de Entrada de PIN Baseada em Software em COTS (SPoC), soluções de Pagamentos sem Contato em COTS (CPoC) e produtos de Pagamentos Móveis em COTS (MPoC).

Parte 2. Resumo Executivo *(continuação)*

Parte 2f. Prestadores de Serviço Terceirizados

O comerciante tem relacionamento com um ou mais prestadores de serviços terceirizados que:

• Armazenam, processam ou transmitem dados da conta em nome do comerciante (por exemplo, gateways de pagamento, processadores de pagamento, prestadores de serviços de pagamento (PSPs, em inglês) e armazenamento externo)	☐ Sim ☐ Não
• Gerenciam componentes do sistema incluídos no escopo da Avaliação (por exemplo, por meio de serviços de controle de segurança de rede, serviços antimalware, gerenciamento de incidentes e eventos de segurança (SIEM, em inglês), centros de contato e atendimento, serviços de hospedagem na web e IaaS, PaaS, SaaS , e provedores de nuvem FaaS)	☐ Sim ☐ Não
• Podem afetar a segurança do CDE do comerciante (por exemplo, prestadores que prestam suporte via acesso remoto e/ou desenvolvedores de software sob medida).	☐ Sim ☐ Não

Se Sim:

Nome do Prestador de Serviços:	**Descrição do(s) Serviço(s) Prestado(s):**

Observação: *O Requisito 12.8 se aplica a todas as entidades nesta lista.*

Parte 2. Resumo Executivo *(continuação)*

Parte 2g. Revisão da Avaliação
(SAQ Seção 2 e apêndices relacionados)

Indique abaixo todas as respostas que foram selecionadas para cada requisito do PCI DSS.

Requisito do PCI DSS	Respostas do Requisito *Mais de uma resposta pode ser selecionada para um determinado requisito. Indique todas as respostas que se aplicam.*				
	Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
Requisito 1:	☐	☐	☐	☐	☐
Requisito 2:	☐	☐	☐	☐	☐
Requisito 3:	☐	☐	☐	☐	☐
Requisito 4:	☐	☐	☐	☐	☐
Requisito 5:	☐	☐	☐	☐	☐
Requisito 6:	☐	☐	☐	☐	☐
Requisito 7:	☐	☐	☐	☐	☐
Requisito 8:	☐	☐	☐	☐	☐
Requisito 9:	☐	☐	☐	☐	☐
Requisito 10:	☐	☐	☐	☐	☐
Requisito 11:	☐	☐	☐	☐	☐
Requisito 12:	☐	☐	☐	☐	☐
Apêndice A2:	☐	☐	☐	☐	☐

Seção 2: Questionário de Autoavaliação D para Comerciantes

Observação: *Os requisitos a seguir refletem os requisitos do documento* Requisitos e Procedimentos de Teste do PCI DSS.

Data de conclusão da autoavaliação: DD-MM-AAAA

Construir e Manter uma Rede e Sistemas Seguros

Requisito 1: Instalar e Manter Controles de Segurança de Rede

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.1 Os processos e mecanismos para instalar e manter os controles de segurança da rede são definidos e compreendidos.							
1.1.1	Todas as políticas e processos operacionais identificados no Requisito 1 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
1.1.2	As funções e responsabilidades para a execução de atividades no Requisito 1 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
1.2 Os controles de segurança de rede (NSCs) são configurados e mantidos.							
1.2.1	Os padrões de configuração para conjuntos de regras NSC são: • Definidos. • Implementados. • Mantidos.	• Examine os padrões de configuração. • Examine as definições de configuração.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.2.2	Todas as mudanças nas conexões de rede e nas configurações dos NSCs são aprovadas e gerenciadas de acordo com o processo de controle de mudanças definido no Requisito 6.5.1.	• Examine os procedimentos documentados. • Examine as configurações de rede. • Examine os registros de controle de mudanças. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade As mudanças nas conexões de rede incluem a adição, remoção ou modificação de uma conexão. As mudanças nas configurações do NSC incluem aquelas relacionadas ao próprio componente, bem como aquelas que afetam a forma como ele desempenha sua função de segurança.						
1.2.3	São mantidos diagramas de rede precisos que mostram todas as conexões entre o CDE e outras redes, incluindo quaisquer redes wireless.	• Examine os diagramas de rede. • Examine as configurações de rede. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Um(ns) diagrama(s) de rede atual ou outra solução técnica ou topológica que identifique conexões e dispositivos de rede pode ser usado para atender a esse requisito.						
1.2.4	Um(s) diagrama(s) de fluxo de dados precisos são mantidos que atendem ao seguinte: • Mostra todos os fluxos de dados da conta entre sistemas e redes. • Atualizado conforme necessário mediante mudanças no ambiente.	• Examine os diagramas de fluxo de dados. • Observe as configurações de rede. • Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Um(s) diagrama(s) de fluxo de dados ou outra solução técnica ou topológica que identifica fluxos de dados de contas em sistemas e redes podem ser usados para atender a esse requisito.						
1.2.5	Todos os serviços, protocolos e portas permitidas são identificados, aprovados e têm uma necessidade comercial definida.	• Examine a documentação. • Examine as definições de configuração.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.2.6	Os recursos de segurança são definidos e implementados para todos os serviços, protocolos e portas em uso e considerados inseguros, de forma que o risco seja mitigado.	• Examine a documentação. • Examine as definições de configuração.	☐	☐	☐	☐	☐
1.2.7	As configurações dos NSCs são revisadas pelo menos uma vez a cada seis meses para confirmar que são relevantes e efetivas.	• Examine os procedimentos documentados. • Examine a documentação das revisões realizadas. • Examine as definições de configuração.	☐	☐	☐	☐	☐
1.2.8	Os arquivos de configuração para o NSCs são: • Protegido contra acesso não autorizado. • Mantido consistente com as configurações de rede ativas.	• Examine os arquivos de configuração do NSC.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Qualquer arquivo ou configuração usado para configurar ou sincronizar os NSCs é considerado um "arquivo de configuração". Isso inclui arquivos, controles automatizados e baseados no sistema, scripts, configurações, infraestrutura como código ou outros parâmetros que são copiados, arquivados ou armazenados remotamente.						
1.3 O acesso à rede de e para o ambiente de dados do titular do cartão é restrito.							
1.3.1	O tráfego de entrada para o CDE é restrito da seguinte forma: • Para apenas o tráfego que é necessário. • Todos os demais tráfegos são especificamente negados.	• Examine os padrões de configuração do NSC. • Examine as configurações do NSC.	☐	☐	☐	☐	☐
1.3.2	O tráfego de saída do CDE é restrito da seguinte forma: • Para apenas o tráfego que é necessário. • Todos os demais tráfegos são especificamente negados.	• Examine os padrões de configuração do NSC. • Examine as configurações do NSC.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.3.3	Os NSCs são instalados entre todas as redes wireless e o CDE, independentemente de a rede sem fio ser um CDE, de modo que: • Todo o tráfego wireless de redes wireless o para o CDE é negado por padrão. • Somente tráfego wireless com finalidade comercial autorizada é permitido no CDE.	• Examine as definições de configuração. • Examine os diagramas de rede.	☐	☐	☐	☐	☐
1.4 As conexões de rede entre redes confiáveis e não confiáveis são controladas.							
1.4.1	Os NSCs são implementados entre redes confiáveis e não confiáveis.	• Examine os padrões de configuração do NSC. • Examine os diagramas de rede atuais • Examine as configurações de rede.	☐	☐	☐	☐	☐
1.4.2	O tráfego de entrada de redes não confiáveis para redes confiáveis é restrito a: • Comunicações com componentes do sistema que estão autorizados a prestar serviços, protocolos e portas acessíveis publicamente. • Respostas com estado para as comunicações iniciadas por componentes do sistema em uma rede confiável. • Todos os demais tráfegos são negados,	• Examine a documentação do NSC. • Examine as configurações do NSC.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O objetivo deste requisito é abordar as sessões de comunicação entre redes confiáveis e não confiáveis, em vez de especificações de protocolos. Este requisito não limita o uso de UDP ou outros protocolos de rede sem conexão se o estado for mantido pelo NSC.						
1.4.3	Medidas antifalsificação são implementadas para detectar e impedir que endereços IP de origem forjados entrem na rede confiável.	• Examine a documentação do NSC. • Examine as configurações do NSC.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.4.4	Os componentes do sistema que armazenam os dados do titular do cartão não podem ser acessados diretamente de redes não confiáveis.	• Examine o diagrama de fluxo de dados e o diagrama de rede. • Examine as configurações do NSC.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica ao armazenamento de dados da conta em memória volátil, mas se aplica onde a memória está sendo tratada como armazenamento persistente (por exemplo, disco RAM). Os dados da conta só podem ser armazenados na memória volátil durante o tempo necessário para dar suporte ao processo de negócios associado (por exemplo, até a conclusão da transação de cartão de pagamento relacionada).						
1.4.5	A divulgação de endereços IP internos e informações de roteamento é limitada apenas a partes autorizadas.	• Examine as configurações do NSC. • Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

Requisito do PCI DSS	Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
		Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
1.5 Os riscos para o CDE de dispositivos de computação que são capazes de se conectar a redes não confiáveis e ao CDE são mitigados.						
1.5.1	Os controles de segurança são implementados em quaisquer dispositivos de computação, incluindo dispositivos de propriedade da empresa e de funcionários, que se conectam a redes não confiáveis (incluindo a Internet) e ao CDE da seguinte forma. • As configurações específicas são definidas para evitar que ameaças sejam introduzidas na rede da entidade. • Os controles de segurança estão funcionando ativamente. • Os controles de segurança não podem ser mudados pelos usuários dos dispositivos de computação, a menos que especificamente documentados e autorizados pela administração, caso a caso, por um período limitado.	• Examine as políticas e os padrões de configuração. • Examine as definições de configuração do dispositivo.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esses controles de segurança podem ser temporariamente desativados apenas se houver necessidade técnica legítima, conforme autorizado pela administração de acordo com o caso. Se esses controles de segurança precisarem ser desabilitados para um propósito específico, deverão ser formalmente autorizados. Medidas de segurança adicionais também podem precisar ser implementadas durante o período em que esses controles de segurança não estiverem ativos. Esse requisito se aplica a dispositivos de computação de propriedade de funcionários e de empresas. Os sistemas que não podem ser gerenciados pela política corporativa apresentam pontos fracos e fornecem oportunidades que podem ser exploradas por indivíduos mal-intencionados.						

Requisito 2: Aplicar as Configurações de Segurança para Todos os Componentes do Sistema

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
2.1 Processos e mecanismos para aplicar configurações seguras a todos os componentes do sistema são definidos e compreendidos.							
2.1.1	Todas as políticas e processos operacionais identificados no Requisito 2 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
2.1.2	As funções e responsabilidades para a execução de atividades no Requisito 2 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
2.2 Os componentes do sistema são configurados para administrar com segurança.							
2.2.1	Os padrões de configuração são desenvolvidos, implementados e mantidos para: • Cobrir todos os componentes do sistema. • Abordar todas as vulnerabilidades de segurança conhecidas. • Ser consistente com os padrões de proteção do sistema aceitos pelo setor ou com as recomendações de proteção do fornecedor. • Ser atualizado conforme novos problemas de vulnerabilidade são identificados, tal como definido no Requisito 6.3.1. • Ser aplicado quando novos sistemas são configurados e verificados como Implementado antes ou imediatamente após um componente do sistema ser conectado a um ambiente de produção.	• Padrões de configuração do sistema. • Revise os padrões de proteção aceitos pelo setor. • Examine as definições de configuração. • Entreviste o pessoal.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
2.2.2	As contas padrão do fornecedor são gerenciadas da seguinte forma: • Se as contas padrão do fornecedor forem usadas, a senha padrão será alterada de acordo com o Requisito 8.3.6. • Se as contas padrão do fornecedor não forem usadas, a conta será removida ou desabilitada.	• Padrões de configuração do sistema. • Examine a documentação do fornecedor. • Observe um administrador do sistema fazendo registro usando as contas padrão do fornecedor. • Examine os arquivos de configuração. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Isso se aplica a TODAS as contas e senhas padrão do fornecedor, incluindo, mas não se limitando a, aquelas usadas por sistemas operacionais, software que preste serviços de segurança, contas de aplicativo e sistema, terminais de ponto de venda (POS), aplicativos de pagamento e padrões de Rede Simples do Protocolo de Gerenciamento (SNMP, por sua sigla em inglês). Este requisito também se aplica quando um componente do sistema não está instalado dentro do ambiente de uma entidade, por exemplo, software e aplicativos que fazem parte do CDE e são acessados por meio de um serviço de assinatura em nuvem.						
2.2.3	As funções primárias que requerem diferentes níveis de segurança são gerenciadas da seguinte forma: • Existe somente uma função primária em um componente do sistema, **OU** • As funções primárias com diferentes níveis de segurança que existem no mesmo componente do sistema são isoladas umas das outras, **OU** • As funções primárias com diferentes níveis de segurança no mesmo componente do sistema são todas protegidas no nível exigido pela função com a mais alta necessidade de segurança.	• Padrões de configuração do sistema. • Examine as configurações do sistema.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
2.2.4	Apenas os serviços, protocolos, daemons e funções necessários são ativados e todas as funcionalidades desnecessárias são removidas ou desativadas.	• Padrões de configuração do sistema. • Examine as configurações do sistema.	☐	☐	☐	☐	☐
2.2.5	Se quaisquer serviços, protocolos ou daemons inseguros estiverem presentes: • A justificativa comercial é documentada. • Recursos de segurança adicionais são documentados e implementados para reduzir o risco de usar serviços, protocolos ou daemons inseguros.	• Examine os padrões de configuração. • Entreviste o pessoal. • Examine as definições de configuração.	☐	☐	☐	☐	☐
2.2.6	Os parâmetros de segurança do sistema são configurados para evitar o uso indevido.	• Padrões de configuração do sistema. • Entreviste o pessoal. • Examine as configurações do sistema.	☐	☐	☐	☐	☐
2.2.7	Todo o acesso administrativo fora do console é criptografado usando criptografia forte.	• Padrões de configuração do sistema. • Observe um registro de administrador. • Examine as configurações do sistema. • Examine a documentação do fornecedor. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Inclui acesso administrativo por meio de interfaces baseadas em navegador e interfaces de programação de aplicativos (APIs).						

Requisito do PCI DSS	Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
		Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
2.3 Os ambientes de hardware são configurados para administrar com segurança.						
2.3.1	Para ambientes wireless conectados ao CDE ou transmitindo dados de conta, todos os padrões do fornecedor sem fio são alterados na instalação ou são confirmados como seguros, incluindo, mas não se limitando a: • Chaves de criptografia sem fio padrão. • Senhas ou pontos de acesso wireless. • Padrões SNMP. • Quaisquer outros padrões de fornecedores sem fio relacionados à segurança.	• Examine as políticas e os procedimentos. • Revise a documentação do fornecedor. • Examine as definições de configuração wireless. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Isso inclui, mas não está limitado a, chaves de criptografia sem fio padrão, senhas em pontos de acesso sem fio, padrões SNMP e quaisquer outros padrões de fornecedores sem fio relacionados à segurança.					
2.3.2	Para ambientes wireless conectados ao CDE ou transmitindo dados da conta, as chaves de criptografia wireless são alteradas da seguinte forma: • Sempre que pessoal com conhecimento da chave deixa a empresa ou a função para a qual o conhecimento era necessário. • Sempre que houver suspeita ou comprovação de que uma chave está comprometida.	• Examine a documentação de gerenciamento de chaves. • Entreviste o pessoal.	☐	☐	☐	☐	☐

Proteger os Dados da Conta

Requisito 3: Proteger os Dados Armazenados da Conta

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.1 Os processos e mecanismos para proteger os dados da conta armazenados são definidos e compreendidos.							
3.1.1	Todas as políticas e processos operacionais identificados no Requisito 3 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
3.1.2	As funções e responsabilidades para a execução de atividades no Requisito 3 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.2 O armazenamento de dados da conta é mínimo.							
3.2.1	O armazenamento de dados da conta é reduzido ao mínimo por meio da implementação de políticas, procedimentos e processos de retenção e descarte de dados que incluem pelo menos o seguinte: • Cobertura para todos os locais de dados de conta armazenados. • Cobertura para quaisquer dados de autenticação confidenciais (SAD) armazenados antes da conclusão da autorização. *Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes.* • Limitar a quantidade de armazenamento de dados e o tempo de retenção ao que é necessário para requisitos jurídicos ou regulamentares e/ou de negócios. • Requisitos de retenção específicos para dados de contas armazenados que definem a duração do período de retenção e incluem uma justificativa de negócios documentada. • Processos para exclusão segura ou processamento de dados da conta irrecuperáveis quando não são mais necessários de acordo com a política de retenção. • Um processo para verificar, pelo menos uma vez a cada três meses, se os dados da conta armazenados que excedem o período de retenção definido foram excluídos com segurança ou tornaram-se irrecuperáveis. *(continuação)*	• Examine as políticas, procedimentos e processos de retenção e descarte de dados. • Entreviste o pessoal. • Examine os arquivos e registros do sistema nos componentes do sistema onde os dados da conta estão armazenados. • Observe os mecanismos usados para tornar os dados da conta irrecuperáveis.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
	Observações de Aplicabilidade						
	Onde os dados da conta são armazenados por um TPSP (por exemplo, em um ambiente de nuvem), as entidades são responsáveis por trabalhar com seus prestadores de serviços para entender como o TPSP atende a esse requisito para a entidade. As considerações incluem garantir que todas as instâncias geográficas de um elemento de dados sejam excluídas com segurança. *O marcador acima (para a cobertura do SAD armazenado antes da conclusão da autorização) é uma prática recomendada até 31 de março de 2025, após o qual será exigido como parte do Requisito 3.2.1 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
3.3 Os dados de autenticação confidenciais (SAD) não são armazenados após a autorização.							
3.3.1	O SAD não é armazenado após a autorização, mesmo se criptografado. Todos os dados de autenticação confidenciais recebidos são tornados irrecuperáveis após a conclusão do processo de autorização.	• Examine as políticas e procedimentos documentados. • Examine as configurações do sistema. • Observe os processos seguros de exclusão de dados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Parte desta Observação de Aplicabilidade foi removida intencionalmente para este SAQ, pois não se aplica a avaliações dos comerciantes. Os dados de autenticação confidenciais incluem os dados citados nos Requisitos 3.3.1.1 a 3.3.1.3.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.3.1.1	O conteúdo completo de qualquer rastreamento não é armazenado após a conclusão do processo de autorização.	• Examine as fontes de dados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	No curso normal dos negócios, os seguintes elementos de dados do rastreamento podem precisar ser retidos: • Nome do Titular do Cartão. • Número da Conta Principal (PAN). • Data de Validade. • Código do Serviço. Para minimizar o risco, armazene com segurança apenas esses elementos de dados conforme necessário para os negócios.						
3.3.1.2	O código de verificação do cartão não é armazenado após a conclusão do processo de autorização.	• Examine as fontes de dados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	O código de verificação do cartão é o número de três ou quatro dígitos impresso na frente ou no verso de um cartão de pagamento usado para verificar transações com cartão não presente.						
3.3.1.3	O número de identificação pessoal (PIN) e o bloqueio de PIN não são armazenados após a conclusão do processo de autorização.	• Examine as fontes de dados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Os bloqueios de PIN são criptografados durante o curso natural dos processos de transação, mas mesmo se uma entidade criptografar o bloqueio de PIN novamente, este ainda não poderá ser armazenado após a conclusão do processo de autorização.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.3.2	O SAD que é armazenado eletronicamente antes da conclusão da autorização é criptografado usando criptografia forte.	• Examine os armazenamentos de dados e as configurações do sistema. • Examine a documentação do fornecedor.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Se o SAD tem permissão para ser armazenado antes da autorização ser determinada pelas organizações que gerenciam programas de conformidade (por exemplo, bandeiras de pagamento e adquirentes). Contate as organizações de interesse para todos os critérios adicionais. Contate estas organizações para todos os critérios adicionais. Este requisito se aplica a todo o armazenamento do SAD, mesmo se nenhum PAN estiver presente no ambiente. Consulte o Requisito 3.2.1 para um requisito adicional que se aplica se o SAD for armazenado antes da conclusão da autorização. *Parte desta Observação de Aplicabilidade foi removida intencionalmente para este SAQ, pois não se aplica a avaliações dos comerciantes.* Esse requisito não substitui como os bloqueios de PIN devem ser gerenciados, nem significa que um bloqueio de PIN criptografado corretamente precisa ser criptografado novamente. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
3.3.3	***Requisito adicional para emissores e empresas que oferecem suporte a serviços de emissão e armazenam dados de autenticação confidenciais.***						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.4 O acesso a telas de PAN completo e a capacidade de copiar o PAN são restritos.							
3.4.1	O PAN é mascarado quando exibido (o PIN e os quatro últimos dígitos são o número máximo de dígitos a serem exibidos), de forma que apenas o pessoal com uma necessidade comercial legítima pode ver mais do que o PIN e os quatro últimos dígitos do PAN.	• Examine as políticas e procedimentos documentados. • Examine as configurações do sistema. • Examine a lista documentada de funções que precisam acessar mais do que o PIN e os últimos quatro dígitos do PAN (inclui o PAN completo). • Examine as exibições do PAN (por exemplo, na tela, em recibos em papel).	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esse requisito não substitui os requisitos mais rígidos em vigor para exibição de dados do titular do cartão - por exemplo, requisitos jurídicos ou de bandeira de pagamento para recibos de ponto de venda (POS). Este requisito se refere à proteção do PAN onde ele é exibido nas telas, recibos de papel, impressões, etc., e não deve ser confundido com o Requisito 3.5.1 para proteção do PAN quando armazenado, processado ou transmitido.						
3.4.2	Ao usar tecnologias de acesso remoto, os controles técnicos evitam a cópia e/ou realocação do PAN para todo o pessoal, exceto para aqueles com autorização explícita documentada e uma necessidade comercial legítima definida.	• Examine as políticas e procedimentos documentados e evidências documentadas para controles técnicos. • Examine as configurações para tecnologias de acesso remoto. • Observe os processos. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Armazenar ou realocar PAN em discos rígidos locais, mídia eletrônica removível e outros dispositivos de armazenamento traz esses dispositivos para o escopo do PCI DSS. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.5 O número da conta principal (PAN, por sua sigla em inglês) é protegido onde quer que seja armazenado.							
3.5.1	O PAN é tornado ilegível em qualquer lugar em que esteja armazenado usando qualquer uma das seguintes abordagens: • Hashes unilaterais baseados em criptografia forte de todo o PAN. • Se o PAN for armazenado, processado, transmitido ou de outra forma presente, os requisitos deste módulo se aplicam além dos Requisitos Principais do Software Seguro. – Se versões hash e truncadas do mesmo PAN, ou diferentes formatos de truncamento do mesmo PAN, estiverem presentes em um ambiente, controles adicionais serão implementados de forma que as diferentes versões não possam ser correlacionadas para reconstruir o PAN original • Tokens de índice. • Esta tabela não pretende ser exaustiva, mas é apresentada para ilustrar os diferentes tipos de requisitos que se aplicam a cada elemento de dados.	• Examine a documentação sobre o sistema usado para tornar o PAN ilegível. • Examine os repositórios de dados. • Examine os registros de auditoria, incluindo registros de aplicativos de pagamento. • Examine os controles para verificar se os PANs com hash e truncados não podem ser correlacionados para reconstruir o PAN original.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a PANs armazenados em armazenamento primário (bancos de dados ou arquivos simples, como planilhas de arquivos de texto), bem como armazenamento não primário (backup, logs de auditoria, exceção ou logs de solução de problemas). Este requisito não impede o uso de arquivos temporários contendo PAN de texto simples durante a criptografia e descriptografia do PAN.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.5.1.1	Os hashes usados para tornar o PAN ilegível (de acordo com o primeiro item do Requisito 3.5.1) são hashes criptográficos com chave de todo o PAN, com processos e procedimentos de gerenciamento de chaves associados, de acordo com os Requisitos 3.6 e 3.7.	• Examine a documentação sobre o método de hash usado. • Examine a documentação sobre os procedimentos e processos de gerenciamento de chaves. • Examine os repositórios de dados. • Examine os registros de auditoria, incluindo registros de aplicativos de pagamento.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Todas as Observações de Aplicabilidade para o Requisito 3.5.1 também se aplicam a este requisito. Os processos e procedimentos de gerenciamento de chaves (Requisitos 3.6 e 3.7) não se aplicam aos componentes do sistema usados para gerar hashes com chave individuais de um PAN para comparação com outro sistema se: • Os componentes do sistema só têm acesso a um valor hash por vez (os valores hash não são armazenados no sistema) **E** • Não há outros dados de conta armazenados no mesmo sistema que os hashes. *Este requisito é considerado uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS. Este requisito substituirá o marcador do Requisito 3.5.1 para hashes unidirecionais assim que sua data de vigência for atingida.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.5.1.2	Se a criptografia em nível de disco ou em nível de partição (em vez de criptografia de banco de dados em nível de arquivo, coluna ou campo) for usada para tornar o PAN ilegível, ela será implementada apenas da seguinte maneira: • Em mídia eletrônica removível. **OU** • Se usado para mídia eletrônica não removível, o PAN também se torna ilegível por meio de outro mecanismo que atenda ao Requisito 3.5.1.	• Observe os processos de criptografia. • Examine as configurações e/ou a documentação do fornecedor. • Observe os processos de criptografia.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a qualquer método de criptografia que forneça PAN em texto não criptografado automaticamente quando um sistema é executado, mesmo que um usuário autorizado não tenha solicitado especificamente esses dados. Embora a criptografia de disco ou de partição ainda possa estar presente nesses tipos de dispositivos, não pode ser o único mecanismo usado para proteger o PAN armazenado nesses sistemas. Qualquer PAN armazenado também deve ser tornado ilegível de acordo com o Requisito 3.5.1 - por exemplo, por meio de truncamento ou um mecanismo de criptografia de nível de dados. A criptografia de disco completo ajuda a proteger os dados em caso de perda física de um disco e, portanto, seu uso é apropriado apenas a dispositivos de armazenamento de mídia eletrônica removíveis. A mídia que faz parte de uma arquitetura de centro de dados (por exemplo, unidades aspiradas a quente, backups de fita em massa) é considerada mídia eletrônica não removível para a qual o Requisito 3.5.1 se aplica. As implementações de criptografia de disco ou partição também devem atender a todos os outros requisitos de criptografia do PCI DSS e gerenciamento de chaves. *Parte desta Observação de Aplicabilidade foi removida intencionalmente para este SAQ, pois não se aplica a avaliações dos comerciantes.* *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.5.1.3	Se a criptografia em nível de disco ou partição for usada (em vez de criptografia de banco de dados em nível de arquivo, coluna ou campo) para tornar o PAN ilegível, ela será gerenciada da seguinte maneira: • O acesso lógico é gerenciado separadamente e independentemente da autenticação do sistema operacional nativo e dos mecanismos de controle de acesso. • As chaves de descriptografia não estão associadas a contas de usuário. • Os fatores de autenticação (senhas, frases secretas ou chaves criptográficas) que permitem o acesso a dados não criptografados são armazenados com segurança.	• Examine as configurações do sistema. • Observe o processo de autenticação. • Examine os arquivos que contêm fatores de autenticação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade As implementações de criptografia de disco ou partição também devem atender a todos os outros requisitos de criptografia do PCI DSS e gerenciamento de chaves.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.6 As chaves criptográficas usadas para proteger os dados armazenados da conta são protegidas.							
3.6.1	Os procedimentos são definidos e implementados para proteger as chaves criptográficas usadas para proteger os dados da conta armazenados contra divulgação e uso indevido que incluem: • O acesso às chaves é restrito ao menor número de guardiães necessários. • As chaves de criptografia de chave são pelo menos tão fortes quanto as chaves de criptografia de dados que protegem. • As chaves de criptografia de chave são armazenadas separadamente das chaves de criptografia de dados. • As chaves são armazenadas com segurança no menor número possível de locais e formas.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a chaves usadas para proteger dados da conta armazenados e a chaves de criptografia de chaves usadas para proteger chaves de criptografia de dados. O requisito para proteger as chaves usadas para proteger os dados armazenados da conta contra divulgação e uso indevido se aplica às chaves de criptografia de dados e às chaves de criptografia de chave. Como uma chave de criptografia de chave pode conceder acesso a muitas chaves de criptografia de dados, as chaves de criptografia de chave requerem fortes medidas de proteção.						
3.6.1.1	*Requisito adicional apenas para prestadores de serviços.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.6.1.2	As chaves secretas e privadas usadas para proteger os dados da conta armazenados são armazenadas em um (ou mais) dos seguintes formulários o tempo todo: • Criptografado com uma chave de criptografia de chave que é pelo menos tão forte quanto a chave de criptografia de dados e que é armazenada separadamente da chave de criptografia de dados. • Dentro de um dispositivo criptográfico seguro (SCD), como um módulo de segurança de hardware (HSM) ou dispositivo de ponto de interação aprovado pelo PTS. • Como pelo menos dois componentes-chave completos ou partes-chave, de acordo com um método aceito pela indústria.	• Examine os procedimentos documentados. • Examine as configurações do sistema e os locais de armazenamento de chaves, inclusive para chaves de criptografia de chaves.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Não é necessário que as chaves públicas sejam armazenadas em um desses formulários. As chaves criptográficas armazenadas como parte de um sistema de gerenciamento de chaves (KMS) que emprega SCDs são aceitáveis. Uma chave criptográfica dividida em duas partes não atende a esse requisito. Chaves secretas ou privadas armazenadas como componentes-chave ou compartilhamentos de chaves devem ser geradas por meio de um dos seguintes: • Usando um gerador de números aleatórios aprovado e dentro de um SCD, **OU** • De acordo com a ISO 19592 ou padrão da indústria equivalente para geração de compartilhamentos de chave secreta.						
3.6.1.3	O acesso aos componentes da chave criptográfica de texto não criptografado é restrito ao menor número de custodiantes necessários.	• Examine as listas de acesso do usuário.	☐	☐	☐	☐	☐
3.6.1.4	As chaves criptográficas são armazenadas no menor número possível de locais.	• Examine os locais de armazenamento de chaves. • Observe os processos.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.7 Onde a criptografia é usada para proteger os dados armazenados da conta, os processos e procedimentos de gerenciamento de chave cobrindo todos os aspectos do ciclo de vida da chave são definidos e implementados.							
3.7.1	Políticas e procedimentos de gerenciamento de chaves são implementados para incluir a geração de chaves criptográficas fortes usadas para proteger os dados armazenados da conta.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Observe o método de geração de chaves.	☐	☐	☐	☐	☐
3.7.2	Políticas e procedimentos de gerenciamento de chaves são implementados para incluir a distribuição segura de chaves criptográficas usadas para proteger os dados armazenados da conta.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Observe o método de distribuição de chaves.	☐	☐	☐	☐	☐
3.7.3	Políticas e procedimentos de gerenciamento de chaves são implementados para incluir armazenamento seguro de chaves criptográficas usadas para proteger dados de contas armazenados.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Observe o método de armazenamento de chaves.	☐	☐	☐	☐	☐
3.7.4	As políticas e procedimentos de gerenciamento de chaves são implementados para alterações de chave criptográfica para chaves que atingiram o fim de seu período criptográfico, conforme definido pelo fornecedor do aplicativo associado ou proprietário da chave e com base nas práticas recomendadas e diretrizes do setor, incluindo o seguinte: • Um criptoperíodo definido para cada tipo de chave em uso. • Um processo para mudanças importantes no final do criptoperíodo definido.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Entreviste o pessoal. • Observe os locais de armazenamento das chaves.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.7.5	Os procedimentos das políticas de gerenciamento de chaves são implementados para incluir a retirada, substituição ou destruição das chaves usadas para proteger os dados armazenados da conta, conforme considerado necessário quando: • A chave atingiu o fim de seu criptoperíodo definido. • A integridade da chave foi enfraquecida, inclusive quando o pessoal com conhecimento de um componente chave de texto não criptografado deixa a empresa ou a função para a qual o componente chave era conhecido. • A chave é suspeita ou conhecida por estar comprometida. Chaves retiradas ou substituídas não são usadas para operações de criptografia.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Se as chaves criptográficas retiradas ou substituídas precisarem ser retidas, essas chaves devem ser arquivadas com segurança (por exemplo, usando uma chave de criptografia de chave).						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
3.7.6	Onde as operações manuais de gerenciamento de chaves criptográficas em texto não criptografado são realizadas por pessoal, as políticas e procedimentos de gerenciamento de chaves são implementados, incluindo o gerenciamento dessas operações usando conhecimento dividido e controle duplo.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Entreviste o pessoal. • Observe os processos.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esse controle é aplicável para operações manuais de gerenciamento de chaves ou onde o gerenciamento de chaves. Uma chave criptográfica que é dividida simplesmente em duas partes não atende a esse requisito. Chaves secretas ou privadas armazenadas como componentes-chave ou compartilhamentos de chaves devem ser geradas por meio de um dos seguintes: • Usando um gerador de número aleatório aprovado e dentro de um dispositivo criptográfico seguro (SCD), como um módulo de segurança de hardware (HSM) ou dispositivo de ponto de interação aprovado pelo PTS, **OU** • De acordo com a ISO 19592 ou padrão da indústria equivalente para geração de compartilhamentos de chave secreta.						
3.7.7	As políticas e procedimentos de gerenciamento de chaves são implementados para incluir a prevenção da substituição não autorizada de chaves criptográficas.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Entreviste o pessoal. • Observe os processos.	☐	☐	☐	☐	☐
3.7.8	As políticas e procedimentos de gerenciamento de chaves são implementados para incluir que os custodiantes das chaves criptográficas reconheçam formalmente (por escrito ou eletronicamente) que compreendem e aceitam suas responsabilidades de custódia das chaves.	• Examine as políticas e procedimentos documentados de gerenciamento de chaves. • Revise a documentação ou outras evidências de reconhecimentos do custodiante principal.	☐	☐	☐	☐	☐
3.7.9	*Requisito adicional apenas para prestadores de serviços.*						

Requisito 4: Proteger os Dados do Titular do Cartão com Criptografia Forte Durante a Transmissão em Redes Públicas Abertas

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
4.1 Processos e mecanismos para proteger os dados do titular do cartão com criptografia forte durante a transmissão em redes públicas abertas são definidos e entendidos.							
4.1.1	Todas as políticas e processos operacionais identificados no Requisito 4 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
4.1.2	As funções e responsabilidades para a execução de atividades no Requisito 4 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
4.2 O PAN é protegido com criptografia forte durante a transmissão.							
4.2.1	Fortes protocolos de criptografia e segurança são implementados da seguinte forma para proteger o PAN durante a transmissão em redes públicas abertas:						
	• Somente chaves e certificados confiáveis são aceitos.	• Examine as políticas e procedimentos documentados. • Entreviste o pessoal. • Examine as configurações do sistema. • Examine as transmissões de dados do titular do cartão. • Examine as chaves e os certificados.	☐	☐	☐	☐	☐
	• Os certificados usados para proteger o PAN durante a transmissão em redes públicas abertas são confirmados como válidos e não expiraram ou foram revogados. *Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes.*		☐	☐	☐	☐	☐
	• O protocolo em uso oferece suporte apenas a versões ou configurações seguras e não oferece suporte a falhas ou uso de versões, algoritmos, tamanhos de chave ou implementações inseguros.		☐	☐	☐	☐	☐
	• A força da criptografia é apropriada para a metodologia de criptografia em uso.		☐	☐	☐	☐	☐
	Observações de Aplicabilidade Um certificado autoassinado também pode ser aceitável se o certificado for emitido por um CA interno da organização, o autor do certificado for confirmado e o certificado for verificado - por exemplo, por meio de hash ou assinatura - e não tiver expirado. *O item acima (para confirmar que os certificados usados para proteger o PAN durante a transmissão em redes públicas abertas são válidos e não expiraram ou foram revogados) é uma prática recomendada até 31 de março de 2025, após a qual será exigido como parte do Requisito 4.2.1 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
4.2.1.1	Um inventário das chaves e certificados confiáveis da entidade usados para proteger o PAN durante a transmissão é mantido.	• Examine as políticas e procedimentos documentados. • Examine o inventário de chaves e certificados confiáveis.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.						
4.2.1.2	As redes wireless que transmitem PAN ou conectadas ao CDE usam as práticas recomendadas da indústria para implementar criptografia forte para autenticação e transmissão.	• Examine as configurações do sistema.	☐	☐	☐	☐	☐
4.2.2	O PAN é protegido por criptografia forte sempre que enviado por meio de tecnologias de mensagens do usuário final.	• Examine as políticas e procedimentos documentados. • Examine as configurações do sistema e a documentação do fornecedor.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Este requisito também se aplica se um cliente, ou outro terceiro, solicitar que o PAN seja enviado a eles por meio de tecnologias de mensagens do usuário final. Pode haver ocorrências em que uma entidade receba dados não solicitados do titular do cartão por meio de um canal de comunicação inseguro que não se destina à transmissão de dados confidenciais. Nessa situação, a entidade pode escolher incluir o canal no escopo de seu CDE e protegê-lo de acordo com o PCI DSS ou excluir os dados do titular do cartão e implementar medidas para evitar que o canal seja usado para os dados do titular do cartão.						

Manter um Programa de Gestão de Vulnerabilidade

Requisito 5: Proteger Todos os Sistemas e Redes de Software Malicioso

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
5.1 Processos e mecanismos para proteger todos os sistemas e redes de software malicioso são definidos e compreendidos.							
5.1.1	Todas as políticas e processos operacionais identificados no Requisito 5 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
5.1.2	As funções e responsabilidades para a execução de atividades no Requisito 5 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
5.2 O software malicioso (malware) é evitado ou detectado e corrigido.							
5.2.1	Uma(s) solução(ões) antimalware é(são) implantada em todos os componentes do sistema, exceto para os componentes do sistema identificados em avaliações periódicas de acordo com o Requisito 5.2.3, que conclui que os componentes do sistema não correm risco de malware.	• Examine os componentes do sistema. • Examine as avaliações periódicas.	☐	☐	☐	☐	☐
5.2.2	A(s) solução(ões) antimalware implantada(s): • Detecta todos os tipos conhecidos de malware. • Remove, bloqueia ou contém todos os tipos conhecidos de malware.	• Examine a documentação do fornecedor. • Examine as configurações do sistema.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
5.2.3	Quaisquer componentes do sistema que não estejam em risco de malware são avaliados periodicamente para incluir o seguinte: • Uma lista documentada de todos os componentes do sistema que não correm risco de malware. • Identificação e avaliação de ameaças de malware em evolução para esses componentes do sistema. • Confirmação se esses componentes do sistema continuam a não exigir proteção antimalware.	• Examine as políticas e procedimentos documentados. • Entreviste o pessoal. • Examine a lista de componentes do sistema sem risco de malware e compare com os componentes do sistema sem uma solução antimalware implantada.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Os componentes do sistema cobertos por este requisito são aqueles para os quais não há solução antimalware implantada de acordo com o Requisito 5.2.1.						
5.2.3.1	A frequência das avaliações periódicas dos componentes do sistema identificados como sem risco de malware é definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	• Examine a análise de risco direcionada. • Examine os resultados documentados das avaliações periódicas. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
5.3 Os mecanismos e processos antimalware são ativos, mantidos e monitorados.							
5.3.1	As soluções antimalware são mantidas atualizadas por meio de atualizações automáticas.	• Examine as configurações da(s) solução(ões) antimalware, incluindo qualquer instalação mestre. • Examine os componentes e registros do sistema	☐	☐	☐	☐	☐
5.3.2	A(s) solução(ões) antimalware: • Executa(m) varreduras periódicas e varreduras ativas ou em tempo real **OU** • Realiza(}m) análise comportamental contínua de sistemas ou processos.	• Examine as configurações da(s) solução(ões) antimalware, incluindo qualquer instalação mestre. • Examine os componentes do sistema • Examine os registros e varre os resultados.	☐	☐	☐	☐	☐
5.3.2.1	Se varreduras de malware periódicas são realizadas para atender ao Requisito 5.3.2, a frequência das varreduras é definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	• Examine a análise de risco direcionada. • Examine os resultados documentados de varreduras periódicas de malware. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a entidades que realizam varreduras periódicas de malware para atender ao Requisito 5.3.2. Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
5.3.3	Para mídia eletrônica removível, a(s) solução(ões) antimalware: • Executa(m) varreduras automáticas de quando a mídia é inserida, conectada ou montada logicamente, **OU** • Realiza(m) análise comportamental contínua de sistemas ou processos quando a mídia é inserida, conectada ou montada logicamente.	• Examine as configurações da(s) solução(ões) antimalware. • Examine os componentes do sistema com mídia eletrônica removível. • Examine os registros e varre os resultados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
5.3.4	Os registros de auditoria da(s) solução(ões) antimalware são habilitados e retidos de acordo com o Requisito 10.5.1.	• Examine as configurações da(s) solução(ões) antimalware.	☐	☐	☐	☐	☐
5.3.5	Os mecanismos antimalware não podem ser desabilitados ou alterados pelos usuários, salvo se especificamente documentados e autorizados pela administração, caso a caso, por um período de tempo limitado.	• Examine as configurações antimalware. • Observe os processos. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade As soluções antimalware podem ser temporariamente desativadas somente se houver uma necessidade técnica legítima, conforme autorizado pela administração caso a caso. Se a proteção antimalware precisar ser desabilitada para uma finalidade específica, ela deverá ser formalmente autorizada. Medidas de segurança adicionais também podem precisar ser implementadas durante o período em que a proteção antimalware não estiver ativa.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
5.4 Os mecanismos antiphishing protegem os usuários contra ataques de phishing.							
5.4.1	Processos e mecanismos automatizados estão em vigor para detectar e proteger o pessoal contra ataques de phishing.	• Observe os processos implementados. • Examine os mecanismos.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O foco deste requisito é proteger a equipe com acesso aos componentes do sistema no escopo do PCI DSS. Atender a este requisito de controles técnicos e automatizados para detectar e proteger o pessoal contra phishing não é o mesmo que o Requisito 12.6.3.1 para treinamento de conscientização de segurança. Atender a esse requisito também não atende ao requisito de fornecer treinamento de conscientização de segurança ao pessoal e vice-versa. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito 6: Desenvolver e Manter Sistemas e Software Seguros

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.1 Os processos e mecanismos para instalar e manter os controles de segurança da rede são definidos e compreendidos.							
6.1.1	Todas as políticas e processos operacionais identificados no Requisito 6 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
6.1.2	As funções e responsabilidades para a execução de atividades no Requisito 6 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
6.2 O software personalizado e sob medida são desenvolvidos com segurança.							
6.2.1	Softwares sob medida e personalizados são desenvolvidos com segurança, da seguinte forma: • Com base nos padrões da indústria e/ou nas práticas recomendadas para desenvolvimento seguro. • De acordo com o PCI DSS (por exemplo, autenticação segura e registro). • Incorporando a consideração de questões de segurança da informação durante cada estágio do ciclo de vida de desenvolvimento de software.	• Examine os procedimentos de desenvolvimento de software documentados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Isso se aplica a todos os softwares desenvolvidos para ou pela entidade para uso próprio da entidade. Inclui software sob medida e personalizado. Não se aplica a software de terceiros.						

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.2.2	A equipe de desenvolvimento de software que trabalha com software sob medida e personalizado é treinada pelo menos uma vez a cada 12 meses da seguinte forma: • Sobre segurança de software relevante para suas funções de trabalho e linguagens de desenvolvimento. • Incluindo design de software seguro e técnicas de codificação seguras. • Incluindo, se ferramentas de teste de segurança são usadas, como usar as ferramentas para detectar vulnerabilidades no software.	• Examine os procedimentos de desenvolvimento de software documentados. • Examine os registros de treinamento. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade A equipe de desenvolvimento de software continua bem informada sobre as práticas seguras de desenvolvimento; segurança de software; e ataques contra as linguagens, estruturas ou aplicativos que eles desenvolvem. O pessoal pode ter acesso a assistência e orientação quando necessário.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.2.3	O software personalizado e sob medida é revisado antes de ser lançado em produção ou para os clientes, para identificar e corrigir vulnerabilidades de codificação em potencial, como segue: • As revisões de código garantem que o código seja desenvolvido de acordo com as diretrizes de codificação seguras. • As revisões de código procuram vulnerabilidades de softwares existentes e emergentes. • As correções apropriadas são implementadas antes do lançamento.	• Examine os procedimentos de desenvolvimento de software documentados. • Entreviste o pessoal responsável. • Examine as evidências de mudanças em software sob medida e personalizado.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito para revisões de código se aplica a todos os softwares sob medida e personalizados (internos e públicos), como parte do ciclo de vida de desenvolvimento do sistema. Os aplicativos da Web voltados para o público também estão sujeitos a controles adicionais para lidar com ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.4 do PCI DSS. As revisões de código podem ser realizadas usando processos manuais ou automatizados ou uma combinação de ambos.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.2.3.1	Se as revisões manuais de código forem realizadas para software sob medida e personalizados antes da liberação para produção, as mudanças de código são: • Revisados por pessoas que não sejam o autor do código de origem e que tenham conhecimento sobre técnicas de revisão de código e práticas seguras de codificação. • Revisados e aprovados pela administração antes do lançamento.	• Examine os procedimentos de desenvolvimento de software documentados. • Entreviste o pessoal responsável. • Examine as evidências de mudanças em software sob medida e personalizado.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade As revisões manuais de código podem ser conduzidas por pessoal interno ou terceirizado experiente. Um indivíduo que recebeu formalmente a responsabilidade pelo controle de liberação e que não é o autor do código original e nem o revisor do código atende aos critérios de gerenciamento.						
6.2.4	Técnicas de engenharia de software ou outros métodos são definidos e usados pelo pessoal de desenvolvimento de software para prevenir ou mitigar ataques de softwares comuns e vulnerabilidades relacionadas em software sob medida e personalizado, incluindo, mas não limitado ao seguinte:						
	• Ataques de injeção, incluindo SQL, LDAP, XPath ou outro comando, parâmetro, objeto, falha ou falhas do tipo injeção.	• Examine os procedimentos documentados. • Entreviste o pessoal responsável pelo desenvolvimento de software.	☐	`☐	☐	☐	☐
	• Ataques a dados e estruturas de dados, incluindo tentativas de manipular buffers, ponteiros, dados de entrada ou dados compartilhados.		☐	☐	☐	☐	☐
	• Ataques ao uso de criptografia, incluindo tentativas de explorar implementações criptográficas fracas, inseguras ou inadequadas, algoritmos, conjuntos de criptografia ou modos de operação. *(continuação)*		☐	☐	☐	☐	☐

Requisito do PCI DSS	Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
		Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
• Ataques à lógica de negócios, incluindo tentativas de abusar ou ignorar recursos e funcionalidades do aplicativo por meio da manipulação de APIs, protocolos e canais de comunicação, funcionalidade do lado do cliente ou outras funções e recursos do sistema/aplicativo. Isso inclui scripts entre sites (XSS) e falsificação de solicitações entre sites (CSRF).		☐	☐	☐	☐	☐
• Ataques a mecanismos de controle de acesso, incluindo tentativas de contornar ou abusar de mecanismos de identificação, autenticação ou autorização, ou tentativas de explorar fraquezas na implementação de tais mecanismos.		☐	☐	☐	☐	☐
• Ataques por meio de qualquer vulnerabilidade de "alto risco" identificada no processo de identificação de vulnerabilidade, conforme definido no Requisito 6.3.1.		☐	☐	☐	☐	☐
Observações de Aplicabilidade						
Isso se aplica a todos os softwares desenvolvidos para ou pela entidade para uso próprio da entidade. Inclui software sob medida e personalizado. Não se aplica a software de terceiros.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.3 Vulnerabilidades de segurança são identificadas e tratadas.							
6.3.1	As vulnerabilidades de segurança são identificadas e gerenciadas da seguinte forma: • Novas vulnerabilidades de segurança são identificadas usando fontes reconhecidas pelo setor para informações de vulnerabilidade de segurança, incluindo alertas de equipes de resposta a emergências de computador (CERTs) internacionais e nacionais. • As vulnerabilidades são atribuídas a uma classificação de risco com base nas práticas recomendadas do setor e na consideração do impacto potencial. • As classificações de risco identificam, no mínimo, todas as vulnerabilidades consideradas de alto risco ou críticas para o ambiente. • Vulnerabilidades para software sob medida e personalizado e de terceiros (por exemplo, sistemas operacionais e bancos de dados) são cobertas.	• Examine as políticas e os procedimentos. • Entreviste o pessoal responsável. • Examine a documentação. • Observe os processos.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não é atendido por, e é além da realização das varreduras de vulnerabilidade em conformidade com os Requisitos 11.3.1 e 11.3.2. Esse requisito é para um processo monitorar ativamente as fontes de mercado de informações de vulnerabilidade e para a entidade determinar a classificação de risco a ser associada a cada vulnerabilidade.						
6.3.2	Um inventário de software sob medida e personalizado e componentes de software de terceiros incorporados ao software sob medida e personalizado é mantido para facilitar o gerenciamento de vulnerabilidades e patches.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.3.3	Todos os componentes do sistema são protegidos contra vulnerabilidades conhecidas, instalando patches/atualizações de segurança aplicáveis da seguinte forma: • Patches/atualizações para as vulnerabilidades críticas (identificados de acordo com o processo de classificação de risco no Requisito 6.3.1) serão instalados dentro de um mês de sua liberação. • Todos os outros patches/atualizações de segurança aplicáveis são instalados dentro de um período de tempo apropriado, conforme determinado pela avaliação da entidade da criticidade do risco para o meio ambiente, conforme identificado de acordo com o processo de classificação de risco no Requisito 6.3.1.	• Examine as políticas e os procedimentos. • Examine os componentes do sistema e o software relacionado. • Compare a lista de patches de segurança instalados com as listas de patches de fornecedores recentes.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.4 Os aplicativos da web voltados para o público são protegidos contra ataques.							
6.4.1	Para aplicativos da web voltados para o público, novas ameaças e vulnerabilidades são abordadas continuamente e esses aplicativos são protegidos contra ataques conhecidos da seguinte forma: • Revisão de aplicativos da web voltados para o público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidade de aplicativos da seguinte maneira: – Pelo menos uma vez a cada 12 meses e após mudanças significativas. – Por uma entidade especializada em segurança de aplicativos. – Incluindo, no mínimo, todos os ataques de softwares comuns no Requisito 6.2.4. – Todas as vulnerabilidades são classificadas de acordo com o Requisito 6.3.1. – Todas as vulnerabilidades são corrigidas. – A aplicação é reavaliada após as correções **OU** • Instalação de solução(ões) técnicas automatizada(s) que continuamente detecta(m) e evita(m) ataques baseados na web da seguinte maneira: – Instalado na frente de aplicativos da Web voltados para o público para detectar e impedir ataques baseados na Web. – Ativamente em execução e atualizado conforme aplicável. – Gerando registros de auditoria. – Configurado para bloquear ataques baseados na web ou gerar um alerta que é investigado imediatamente. *(continuação)*	• Examine os processos documentados. • Entreviste o pessoal. • Examine os registros de avaliações de segurança de aplicativos • Examine as definições de configuração do sistema e os registros de auditoria.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
	Observações de Aplicabilidade Esta avaliação não é igual às varreduras de vulnerabilidade realizadas para os Requisitos 11.3.1 e 11.3.2. Este requisito será substituído pelo Requisito 6.4.2 após 31 de março de 2025, quando o Requisito 6.4.2 entrar em vigor.						
6.4.2	Para aplicativos da web voltados para o público, é implantada uma solução técnica automatizada que detecta e evita continuamente ataques baseados na web, com pelo menos o seguinte: • É instalado na frente de aplicativos da web voltados para o público e está configurado para detectar e prevenir ataques baseados na web. • Ativamente em execução e atualizado conforme aplicável. • Gerando registros de auditoria. • Configurado para bloquear ataques baseados na web ou gerar um alerta que é investigado imediatamente.	• Examine as definições de configuração do sistema. • Examine os registros de auditoria. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este novo requisito substituirá o Requisito 6.4.1 assim que sua data de vigência for atingida. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.4.3	Todos os scripts da página de pagamento que são carregados e executados no navegador do consumidor são gerenciados da seguinte forma:						
	• Um método é implementado para confirmar que cada script está autorizado.	• Examine as políticas e os procedimentos. • Entreviste o pessoal responsável. • Examine os registros de inventário. • Examine as configurações do sistema.	☐	☐	☐	☐	☐
	• Um método é implementado para garantir a integridade de cada script.		☐	☐	☐	☐	☐
	• Um inventário de todos os scripts é mantido com a justificativa de negócio ou técnica por escrito de porque cada um é necessário.		☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a todos os scripts carregados do ambiente da entidade e scripts carregados de terceiros e terceiros indiretos. Este requisito também se aplica a scripts na(s) página(s) da web da entidade que incluam uma página/formulário de pagamento incorporado de um TPSP/processador de pagamento (por exemplo, um ou mais frames ou iframes inline). Este requisito não se aplica a uma entidade para scripts em uma página/formulário de pagamento incorporado de um TPSP/processador de pagamento (por exemplo, um ou mais iframes), onde a entidade inclui uma página/formulário de pagamento de um TPSP/processador de pagamento em sua página da web. Os scripts na página/formulário de pagamento incorporado do TPSP/processador de pagamento são de responsabilidade do TPSP/processador de pagamento para serem gerenciados de acordo com este requisito. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.5 Mudanças em todos os componentes do sistema são administrados com segurança.							
6.5.1	As mudanças em todos os componentes do sistema no ambiente de produção são feitas de acordo com os procedimentos estabelecidos que incluem: • Motivo e descrição da mudança. • Documentação do impacto de segurança. • Aprovação de mudança documentada por partes autorizadas. • Teste para verificar se a mudança não afeta negativamente a segurança do sistema. • Para mudanças de software sob medida e personalizadas, todas as atualizações são testadas quanto à conformidade com o Requisito 6.2.4 antes de serem implantadas em produção. • Procedimentos para resolver falhas e retornar a um estado seguro.	• Examine os procedimentos de controle de mudanças documentados. • Examine as mudanças recentes nos componentes do sistema e rastreie as alterações na documentação de controle de mudanças. • Examine a documentação de controle de mudanças.	☐	☐	☐	☐	☐
6.5.2	Após a conclusão de uma mudanças significativa, todos os requisitos aplicáveis do PCI DSS são confirmados em vigor em todos os sistemas e redes novos ou mudados, e a documentação é atualizada conforme aplicável.	• Examine a documentação para mudanças significativas. • Entreviste o pessoal. • Observe os sistemas/redes afetados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Essas mudanças significativas também devem ser capturadas e refletidas na atividade anual de confirmação do escopo do PCI DSS da entidade de acordo com o Requisito 12.5.2.						
6.5.3	Os ambientes de pré-produção são separados dos ambientes de produção e a separação é aplicada com controles de acesso.	• Examine as políticas e os procedimentos. • Examine a documentação da rede e as configurações dos controles de segurança da rede. • Examine as configurações de controle de acesso.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
6.5.4	Os papeis e funções são separadas entre os ambientes de produção e pré-produção para fornecer responsabilidade de modo que apenas as mudanças revisadas e aprovadas sejam implantadas.	• Examine as políticas e os procedimentos. • Observe os processos. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Em ambientes com pessoal limitado, onde os indivíduos desempenham vários papeis ou funções, esse mesmo objetivo pode ser alcançado com controles de procedimento adicionais que fornecem responsabilidade. Por exemplo, um desenvolvedor também pode ser um administrador que usa uma conta de nível de administrador com privilégios elevados no ambiente de desenvolvimento e, para sua função de desenvolvedor, usa uma conta separada com acesso de nível de usuário ao ambiente de produção.						
6.5.5	Os PANs dinâmicos não são usados em ambientes de pré-produção, exceto onde esses ambientes estão incluídos no CDE e protegidos de acordo com todos os requisitos do PCI DSS aplicáveis.	• Examine as políticas e os procedimentos. • Observe os processos de teste. • Entreviste o pessoal. • Examine os dados de teste de pré-produção.	☐	☐	☐	☐	☐
6.5.6	Os dados e as contas de teste são removidos dos componentes do sistema antes que o sistema entre em produção.	• Examine as políticas e os procedimentos. • Observe os processos de teste para software de prateleira e aplicativos internos. • Entreviste o pessoal. • Examine dados e contas para softwares de prateleira instalados ou atualizados recentemente e aplicativos internos.	☐	☐	☐	☐	☐

Implementar Medidas Fortes de Controle de Acesso

Requisito 7: Restringir o Acesso aos Componentes do Sistema e aos Dados do Titular do Cartão por Necessidade de Conhecimento da Empresa

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
7.1 Processos e mecanismos para restringir o acesso aos componentes do sistema e dados do titular do cartão por necessidade de negócios são definidos e compreendidos.							
7.1.1	Todas as políticas e processos operacionais identificados no Requisito 7 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
7.1.2	As funções e responsabilidades para a execução de atividades no Requisito 7 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
7.2 O acesso aos componentes e dados do sistema é definido e atribuído apropriadamente.							
7.2.1	Um modelo de controle de acesso é definido e inclui a concessão de acesso da seguinte forma: • Acesso apropriado dependendo do negócio da entidade e necessidades de acesso. • Acesso aos componentes do sistema e recursos de dados que se baseiam na classificação e funções do trabalho dos usuários. • O mínimo de privilégios necessários (por exemplo, usuário, administrador) para executar uma função de trabalho.	• Examine as políticas e procedimentos documentados. • Entreviste o pessoal. • Examine as configurações do modelo de controle de acesso.	☐	☐	☐	☐	☐
7.2.2	O acesso é atribuído a usuários, incluindo usuários privilegiados, com base em: • Classificação e função do trabalho. • Menores privilégios necessários para desempenhar as responsabilidades do trabalho.	• Examine as políticas e os procedimentos. • Examine as configurações de acesso do usuário, inclusive para usuários privilegiados. • Entreviste o pessoal de gestão responsável. • Entreviste o pessoal responsável pela atribuição de acesso.	☐	☐	☐	☐	☐
7.2.3	Os privilégios exigidos são aprovados por pessoal autorizado.	• Examine as políticas e os procedimentos. • Examine os IDs de usuário e os privilégios atribuídos. • Examine as aprovações documentadas.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
7.2.4	Todas as contas de usuário e privilégios de acesso relacionados, incluindo contas de terceiros/fornecedores, são analisados da seguinte forma: • Pelo menos uma vez a cada seis meses. • Para garantir que as contas e o acesso do usuário permaneçam apropriados com base na função do trabalho. • Qualquer acesso inadequado é abordado. • A administração reconhece que o acesso continua apropriado.	• Examine as políticas e os procedimentos. • Entreviste o pessoal responsável. • Examine os resultados documentados de revisões periódicas de contas de usuários.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a todas as contas de usuário, incluindo aquelas usadas por funcionários e terceiros/fornecedores, e contas usadas para acessar serviços de nuvem de terceiros. Consulte os Requisitos 7.2.5 e 7.2.5.1 e 8.6.1 a 8.6.3 para obter os controles de aplicativos e contas do sistema. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
7.2.5	Todas as contas de aplicativo e sistema e privilégios de acesso relacionados são atribuídos e gerenciados da seguinte forma: • Com base nos privilégios mínimos necessários para a operabilidade do sistema ou aplicativo. • O acesso é limitado aos sistemas, aplicativos ou processos que requerem especificamente seu uso.	• Examine as políticas e os procedimentos. • Examine os privilégios associados às contas do sistema e do aplicativo • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
7.2.5.1	Todos os acessos por aplicativo e contas de sistema e privilégios de acesso relacionados são revisados da seguinte forma: • Periodicamente (na frequência definida na análise de risco alvo da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1). • O acesso do aplicativo/sistema permanece apropriado para a função que está sendo executada. • Qualquer acesso inadequado é abordado. • A administração reconhece que o acesso continua apropriado.	• Examine as políticas e os procedimentos. • Examine a análise de risco direcionada. • Entreviste o pessoal responsável. • Examine os resultados documentados de revisões periódicas de contas de sistema e aplicativo e privilégios relacionados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
7.2.6	Todo o acesso do usuário a repositórios de consulta de dados armazenados do titular do cartão é restrito da seguinte forma: • Por meio de aplicativos ou outros métodos programáticos, com acesso e ações permitidas com base nas funções do usuário e privilégios mínimos. • Apenas o(s) administrador(es) responsáveis podem acessar ou consultar diretamente os repositórios do CHD armazenado.	• Examine as políticas e os procedimentos. • Entreviste o pessoal. • Examine as definições de configuração para consultar repositórios de dados armazenados do titular do cartão.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica aos controles de acesso do usuário aos repositórios de consulta dos dados armazenados do titular do cartão. Consulte os Requisitos 7.2.5 e 7.2.5.1 e 8.6.1 a 8.6.3 para obter os controles de aplicativos e contas do sistema.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
7.3 O acesso aos componentes e dados do sistema é gerenciado por meio de um(ns) sistema(s) de controle de acesso.							
7.3.1	Um(ns) sistema(s) de controle(s) de acesso está em vigor que restringe(m) o acesso com base na necessidade de um usuário saber e cobre(m) todos os componentes do sistema.	• Examine a documentação do fornecedor. • Examine as definições de configuração.	☐	☐	☐	☐	☐
7.3.2	O(s) sistema(s) de controle de acesso é(são) configurado(s) para fazer cumprir as permissões atribuídas a indivíduos, aplicativos e sistemas com base na classificação e função do trabalho.	• Examine a documentação do fornecedor. • Examine as definições de configuração.	☐	☐	☐	☐	☐
7.3.3	O(s) sistema(s) de controle de acesso é(são) configurado(s) para “negar todos” por padrão.	• Examine a documentação do fornecedor. • Examine as definições de configuração.	☐	☐	☐	☐	☐

Requisito 8: Identificar Usuários e Autenticar o Acesso aos Componentes do Sistema

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.1 Processos e mecanismos para identificar usuários e autenticar o acesso aos componentes do sistema são definidos e compreendidos.							
8.1.1	Todas as políticas e processos operacionais identificados no Requisito 8 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
8.1.2	As funções e responsabilidades pela execução de atividades no Requisito 8 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
8.2 A identificação do usuário e contas relacionadas para usuários e administradores são estritamente gerenciadas ao longo do ciclo de vida de uma conta.							
8.2.1	Todos os usuários recebem um ID exclusivo antes de permitir o acesso aos componentes do sistema ou aos dados do titular do cartão.	• Entreviste o pessoal responsável. • Examine os registros de auditoria e outras evidências.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação.						

Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.2.2	IDs de grupo, compartilhadas ou genéricas ou outras credenciais de autenticação compartilhadas são usadas apenas quando necessário em uma base de exceção e são gerenciadas da seguinte forma: • O uso da ID é evitado, a menos que seja necessário em uma circunstância excepcional. • O uso é limitado ao tempo necessário para a circunstância excepcional. • A justificativa comercial para uso é documentada. • O uso é explicitamente aprovado pela administração. • A identidade do usuário individual é confirmada antes que o acesso a uma conta seja concedido. • Cada ação realizada é atribuível a um usuário individual.	• Examine as listas de contas de usuários nos componentes do sistema e a documentação aplicável. • Examine as políticas e procedimentos de autenticação. • Entreviste os administradores do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação.						
8.2.3	***Requisito adicional apenas para prestadores de serviços.***						
8.2.4	Adição, exclusão e modificação de IDs de usuário, fatores de autenticação e outros objetos identificadores são gerenciados da seguinte forma: • Autorizado com a devida aprovação. • implementado apenas com os privilégios especificados na aprovação documentada.	• Examine as autorizações documentadas em várias fases do ciclo de vida da conta (adições, modificações e exclusões). • Examine as configurações do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a todas as contas de usuário, incluindo funcionários, contratados, consultores, trabalhadores temporários e fornecedores terceirizados.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.2.5	O acesso para usuários desligados é imediatamente revogado.	• Examine as fontes de informações para usuários encerrados. • Revise as listas de acesso de usuários atuais. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
8.2.6	Contas de usuário inativas são removidas ou desabilitadas dentro de 90 dias de inatividade.	• Examine as contas de usuário e as informações do último registro. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
8.2.7	Contas usadas por terceiros para acessar, dar suporte ou manter os componentes do sistema por meio de acesso remoto são gerenciadas da seguinte forma: • Ativado apenas durante o período de tempo necessário e desativado quando não estiver em uso. • O uso é monitorado para atividades inesperadas.	• Entreviste o pessoal responsável. • Examine a documentação para gerenciar contas. • Examine a evidência.	☐	☐	☐	☐	☐
8.2.8	Se uma sessão de usuário ficou inativa por mais de 15 minutos, o usuário deve se autenticar novamente para reativar o terminal ou a sessão.	• Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação. Este requisito não tem como objetivo impedir que atividades legítimas sejam realizadas enquanto o console/PC estiver desacompanhado.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.3 Uma autenticação forte para usuários e administradores é estabelecida e gerenciada.							
8.3.1	Todo o acesso do usuário aos componentes do sistema para usuários e administradores é autenticado por meio de pelo menos um dos seguintes fatores de autenticação: • Algo que você conhece, como uma senha ou frase secreta • Algo que você possui, como um dispositivo de token ou cartão inteligente • Algo que você é, como um elemento biométrico.	• Examine a documentação que descreve os fatores de autenticação usados. • Para cada tipo de fator de autenticação usado com cada tipo de componente do sistema, observe o processo de autenticação.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação. Este requisito não substitui os requisitos de autenticação multifator (MFA), mas se aplica aos sistemas dentro do escopo que não estão sujeitos aos requisitos de MFA. Um certificado digital é uma opção válida para “algo que você tem” se for exclusivo para um usuário específico.						
8.3.2	A criptografia forte é usada para tornar todos os fatores de autenticação ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema.	• Examine a documentação do fornecedor. • Examine os padrões de configuração do sistema. • Examine os repositórios de fatores de autenticação. • Examine as transmissões de dados.	☐	☐	☐	☐	☐
8.3.3	A identidade do usuário é verificada antes de modificar qualquer fator de autenticação.	• Examine os procedimentos para modificar os fatores de autenticação. • Observe o pessoal de segurança.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.3.4	As tentativas de autenticação inválidas são limitadas: • Bloquear o ID do usuário após no máximo 10 tentativas. • Definindo a duração do bloqueio para um mínimo de 30 minutos ou até que a identidade do usuário seja confirmada.	• Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transaçã.						
8.3.5	Se as senhas/frases secretas forem usadas como fatores de autenticação para atender ao Requisito 8.3.1, elas serão definidas e redefinidas para cada usuário da seguinte forma: • Defina um valor exclusivo para o uso pela primeira vez e na reinicialização. • Obrigado a ser mudado imediatamente após o primeiro uso.	• Examine os procedimentos para definir e redefinir senhas/frases secretas. • Observe o pessoal de segurança.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.3.6	Se as senhas/frases secretas forem usadas como fatores de autenticação para atender ao Requisito 8.3.1, elas atendem ao seguinte nível mínimo de complexidade: • Um comprimento mínimo de 12 caracteres (ou SE o sistema não suportar 12 caracteres, um comprimento mínimo de oito caracteres). • Contém caracteres numéricos e alfabéticos.	• Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a: • Contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação. • Contas de aplicativo ou sistema, que são regidas pelos requisitos da seção 8.6. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.* Até 31 de março de 2025, as senhas devem ter no mínimo sete caracteres de acordo com o PCI DSS v3.2.1 Requisito 8.2.3.						
8.3.7	Indivíduos não têm permissão para enviar uma nova senha/frase secreta que seja igual a qualquer uma das últimas quatro senhas/frases secretas usadas.	• Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.3.8	As políticas e procedimentos de autenticação são documentados e comunicados a todos os usuários, incluindo: • Orientação sobre a seleção de fatores de autenticação fortes. • Orientação sobre como os usuários devem proteger seus fatores de autenticação. • Instruções para não reutilizar senhas/frases secretas usadas anteriormente. • Instruções para alterar senhas/frases-senha se houver qualquer suspeita ou conhecimento de que a senha/frases secretas foram comprometidas e como relatar o incidente.	• Examine os procedimentos. • Entreviste o pessoal. • Revise as políticas e procedimentos de autenticação que são distribuídos aos usuários. • Entreviste os usuários.	☐	☐	☐	☐	☐
8.3.9	Se as senhas / frases secretas forem usadas como o único fator de autenticação para o acesso do usuário (ou seja, em qualquer implementação de autenticação de fator único), então: • As senhas/frases secretas são alteradas pelo menos uma vez a cada 90 dias, **OU** • A postura de segurança das contas é analisada dinamicamente e o acesso em tempo real aos recursos é automaticamente determinado em conformidade.	• Inspecione os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica aos componentes do sistema dentro do escopo onde o MFA é usado. Este requisito não se aplica a contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação. Este requisito não se aplica a contas de clientes de prestadores de serviços, mas se aplica a contas para funcionários de prestadores de serviços.						
8.3.10	***Requisito adicional apenas para prestadores de serviços***						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.3.10.1	***Requisito adicional apenas para prestadores de serviços***						
8.3.11	Onde fatores de autenticação, como tokens de segurança físicos ou lógicos, cartões inteligentes ou certificados são usados: • Os fatores são atribuídos a um usuário individual e não são compartilhados entre vários usuários. • Os controles físicos e/ou lógicos garantem que apenas o usuário pretendido pode usar esse fator para obter acesso.	• Examine as políticas e procedimentos de autenticação. • Entreviste o pessoal de segurança. • Examine as definições de configuração do sistema e/ou observe os controles físicos, conforme aplicável.	☐	☐	☐	☐	☐
8.4 A autenticação multifator (MFA) é implementada para proteger o acesso ao CDE.							
8.4.1	O MFA é implementado para todos os acessos não-console no CDE para o pessoal com acesso administrativo.	• Examine as configurações de rede e/ou sistema. • Observe o pessoal do administrador fazendo login no CDE.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O requisito de MFA para acesso administrativo sem console se aplica a todos os funcionários com privilégios elevados ou aumentados acessando o CDE por meio de uma conexão sem console - ou seja, por meio de acesso lógico que ocorre em uma interface de rede em vez de uma conexão física direta.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.4.2	O MFA é implementado para todos os acessos sem console ao CDE.	• Examine as configurações de rede e/ou sistema. • Observe o pessoal fazendo login no CDE. • Examine a evidência.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Este requisito não se aplica a: • Contas de aplicativo ou sistema executando funções automatizadas. • Contas de usuário em terminais de ponto de venda que têm acesso a apenas um número de cartão por vez para facilitar uma única transação (como IDs usados por caixas em terminais de ponto de venda). • Contas de usuário autenticadas apenas com fatores de autenticação resistentes ao phishing. O MFA é necessário para ambos os tipos de acesso especificados nos Requisitos 8.4.2 e 8.4.3. Portanto, a aplicação de MFA a um tipo de acesso não substitui a necessidade de aplicar outra instância de MFA a outro tipo de acesso. Se um indivíduo primeiro se conecta à rede da entidade por meio de acesso remoto e, posteriormente, inicia uma conexão ao CDE de dentro da rede, de acordo com este requisito, o indivíduo se autenticaria usando MFA duas vezes, uma vez ao se conectar por acesso remoto à rede da entidade e uma vez ao conectar-se da rede da entidade ao CDE. Os requisitos de MFA se aplicam a todos os tipos de componentes do sistema, incluindo nuvem, sistemas hospedados e aplicativos locais, dispositivos de segurança de rede, estações de trabalho, servidores e terminais, e incluem acesso direto a redes ou sistemas de uma entidade, bem como com base na web acesso a um aplicativo ou função. O MFA para acesso ao CDE pode ser implementado no nível da rede ou do sistema/aplicativo; não precisa ser aplicado em ambos os níveis. Por exemplo, se o MFA for usado quando um usuário se conecta à rede CDE, ele não precisa ser usado quando o usuário efetua login em cada sistema ou aplicativo no CDE. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*					

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.4.3	O MFA é implementado para todos os acessos remotos originados de fora da rede da entidade que podem acessar ou impactar o CDE.	• Examine as configurações de rede e/ou sistema para servidores e sistemas de acesso remoto. • Observe o pessoal (por exemplo, usuários e administradores) e terceiros conectando-se remotamente à rede.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	O requisito de MFA para acesso remoto originado de fora da rede da entidade se aplica a todas as contas de usuário que podem acessar a rede remotamente, onde esse acesso remoto leva ou pode levar ao acesso ao CDE. Isto inclui todo o acesso remoto por pessoal (usuários e administradores) e terceiros (incluindo, mas não limitado a, vendedores, fornecedores, prestadores de serviços e clientes). Se o acesso remoto for a uma parte da rede da entidade que está devidamente segmentada do CDE, de modo que os usuários remotos não possam acessar ou impactar o CDE, o MFA para acesso remoto a essa parte da rede não é necessário. Todavia, o MFA é necessário para qualquer acesso remoto às redes com acesso ao CDE e é recomendado para todos os acessos remotos às redes da entidade. Os requisitos de MFA se aplicam a todos os tipos de componentes de sistema, incluindo nuvem, sistemas hospedados e aplicativos locais, dispositivos de segurança de rede, estações de trabalho, servidores e terminais, e incluem acesso direto a redes ou sistemas de uma entidade, bem como com base na web acesso a um aplicativo ou função.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.5 Os sistemas de autenticação multifator (MFA) são configurados para evitar o uso indevido.							
8.5.1	Os sistemas MFA são implementados da seguinte forma: • O sistema MFA não é suscetível a ataques de repetição. • Os sistemas MFA não podem ser contornados por nenhum usuário, incluindo usuários administrativos, a menos que especificamente documentado e autorizado pela administração de forma excepcional, por um período de tempo limitado. • São usados pelo menos dois tipos diferentes de fatores de autenticação. • O sucesso de todos os fatores de autenticação é necessário antes que o acesso seja concedido. **Observações de Aplicabilidade** *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*	• Examine a documentação do sistema do fornecedor. • Examine as configurações do sistema para a implementação do MFA. • Entreviste o pessoal responsável e observe os processos. • Observe o pessoal fazendo login nos componentes do sistema no CDE. • Observe o pessoal se conectando remotamente de fora da rede da entidade.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.6 O uso de contas de aplicativo e sistema e fatores de autenticação associados são estritamente gerenciados.							
8.6.1	Se as contas usadas por sistemas ou aplicativos puderem ser usadas para login interativo, elas serão gerenciadas da seguinte forma: • O uso interativo é evitado, a menos que seja necessário em uma circunstância excepcional. • O uso interativo é limitado ao tempo necessário para a circunstância excepcional. • A justificativa comercial para uso interativo é documentada. • O uso interativo é explicitamente aprovado pela administração. • A identidade do usuário individual é confirmada antes que o acesso a uma conta seja concedido. • Cada ação realizada é atribuível a um usuário individual.	• Examine as contas do aplicativo e do sistema que podem ser usadas para login interativo. • Entreviste o pessoal administrativo.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.6.2	As senhas/frases secretas para qualquer aplicativo e contas do sistema que podem ser usadas para login interativo não são codificadas em scripts, arquivos de configuração/propriedade ou código-fonte personalizado e sob medida.	• Entreviste o pessoal. • Examine os procedimentos de desenvolvimento do sistema. • Examine os scripts, arquivos de configuração/propriedade e código-fonte personalizado e sob medida para contas de aplicativos e sistemas que podem ser usados para login interativo.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	As senhas/frases secretas armazenadas devem ser criptografadas de acordo com o Requisito 8.3.2 do PCI DSS. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
8.6.3	As senhas/frases secretas para qualquer aplicativo e contas do sistema são protegidas contra o uso indevido, como se segue: • As senhas/frases secretas são alteradas periodicamente (na frequência definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1) e sob suspeita ou confirmação de comprometimento. • As senhas/frases secretas são construídas com complexidade suficiente apropriada para a frequência com que a entidade altera as senhas/frases secretas.	• Examine as políticas e os procedimentos. • Examine a análise de risco direcionada. • Entreviste o pessoal responsável. • Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito 9: Restringir o Acesso Físico aos Dados do Titular do Cartão

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.1 Os processos e mecanismos para restringir o acesso físico aos dados do titular do cartão são definidos e compreendidos.							
9.1.1	Todas as políticas e processos operacionais identificados no Requisito 9 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
9.1.2	As funções e responsabilidades para a execução de atividades no Requisito 9 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
9.2 Os controles de acesso físico gerenciam a entrada em instalações e sistemas que contêm dados do titular do cartão.							
9.2.1	Controles apropriados de entrada nas instalações estão em vigor para restringir o acesso físico aos sistemas no CDE.	• Observe os controles de entrada física. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito não se aplica a locais de acesso público aos consumidores (titulares de cartão).						

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.2.1.1	O acesso físico individual a áreas sensíveis dentro do CDE é monitorado com câmeras de vídeo ou mecanismos de controle de acesso físico (ou ambos) da seguinte forma: • Os pontos de entrada e saída de/para áreas sensíveis dentro do CDE são monitorados. • Os dispositivos ou mecanismos de monitoramento são protegidos contra adulteração ou desativação. • Os dados coletados são revisados e correlacionados com outras entradas. • Os dados coletados são armazenados por pelo menos três meses, a menos que de outra forma restrito por lei.	• Observe os locais onde ocorre o acesso físico individual a áreas sensíveis dentro do CDE. • Observe os mecanismos de controle de acesso físico e/ou examine as câmeras de vídeo. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
9.2.2	Controles físicos e/ou lógicos são implementados para restringir o uso de tomadas de rede acessíveis ao público dentro da instalação.	• Entreviste o pessoal responsável. • Observe os locais das tomadas de rede acessíveis ao público.	☐	☐	☐	☐	☐
9.2.3	O acesso físico a pontos de acesso wireless, gateways, hardware de rede/comunicação e linhas de telecomunicações dentro da instalação é restrito.	• Entreviste o pessoal responsável. • Observe as localizações de hardware e as linhas.	☐	☐	☐	☐	☐
9.2.4	O acesso aos consoles em áreas sensíveis é restrito por meio de bloqueio quando não estiver em uso.	• Observe a tentativa de um administrador do sistema de fazer login em consoles em áreas sensíveis.	☐	☐	☐	☐	☐
9.3 O acesso físico para pessoal e visitantes é autorizado e gerenciado							
9.3.1	Procedimentos são implementados para autorizar e gerenciar o acesso físico do pessoal ao CDE, incluindo: • Identificação de pessoal. • Gerenciar mudanças nos requisitos de acesso físico de um indivíduo. • Revogar ou encerrar a identificação de pessoal. • Limitar o acesso ao processo ou sistema de identificação ao pessoal autorizado.	• Examine os procedimentos documentados. • Observe os métodos de identificação, como crachás de identificação. • Observe os processos.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.3.1.1	O acesso físico às áreas sensíveis dentro do CDE para o pessoal é controlado da seguinte forma: • O acesso é autorizado e baseado na função de trabalho individual. • O acesso é revogado imediatamente após o encerramento. • Todos os mecanismos de acesso físico, como chaves, cartões de acesso, etc., são devolvidos ou desabilitados na rescisão.	• Observe o pessoal em áreas sensíveis dentro do CDE. • Entreviste o pessoal responsável. • Examine as listas de controle de acesso físico. • Observe os processos.	☐	☐	☐	☐	☐
9.3.2	Procedimentos são implementados para autorizar e gerenciar o acesso de visitantes ao CDE, incluindo: • Os visitantes são autorizados antes de entrar. • Os visitantes são sempre acompanhados. • Os visitantes são claramente identificados e recebem um crachá ou outra identificação que expira. • Crachás de visitante ou outra identificação distingue visivelmente visitantes de funcionários.	• Examine os procedimentos documentados. • Observe os processos quando os visitantes estão presentes no CDE. • Entreviste o pessoal. • Observe o uso de crachás de visitante ou outra identificação.	☐	☐	☐	☐	☐
9.3.3	Crachás ou identificação de visitante são entregues ou desativados antes de os visitantes deixarem as instalações ou na data de expiração.	• Observe os visitantes saindo da instalação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
9.3.4	Registro de visitantes são usados para manter um registro físico da atividade tanto do visitante dentro da instalação como dentro de áreas sensíveis, incluindo: • O nome do visitante e a organização representada. • A data e hora da visita. • O nome do pessoal que autoriza o acesso físico. • Reter o registro por pelo menos três meses, a menos que seja restringido de outra forma por lei.	• Examine os registros de visitantes. • Entreviste o pessoal responsável. • Examine os locais de armazenamento dos registros de visitantes.	☐	☐	☐	☐	☐
9.4 A mídia com os dados do titular do cartão é armazenada, acessada, distribuída e destruída com segurança.							
9.4.1	Todas as mídias com dados do titular do cartão são fisicamente protegidas.	• Examine a documentação.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.4.1.1	Os backups de mídia off-line com os dados do titular do cartão são armazenados em um local seguro.	• Examine os procedimentos documentados. • Examine os registros ou outra documentação. • Entreviste o pessoal responsável no(s) local(is) de armazenamento.	☐	☐	☐	☐	☐
9.4.1.2	A segurança do(s) local(is) de backup de mídia off-line com os dados do titular do cartão é revisada pelo menos uma vez a cada 12 meses.	• Examine os procedimentos documentados, registros ou outra documentação. • Entreviste o pessoal responsável no(s) local(is) de armazenamento.	☐	☐	☐	☐	☐
9.4.2	Todas as mídias com dados do titular do cartão são classificadas de acordo com a sensibilidade dos dados.	• Examine os procedimentos documentados. • Examine os registros de mídia ou outra documentação.	☐	☐	☐	☐	☐
9.4.3	A mídia com os dados do titular do cartão enviada para fora da instalação é protegida da seguinte forma: • A mídia enviada para fora da instalação é registrada. • A mídia é enviada por correio seguro ou outro método de entrega que possa ser rastreada com precisão. • Os registros de rastreamento externo incluem detalhes sobre a localização da mídia.	• Examine os procedimentos documentados. • Entreviste o pessoal. • Examine os registros. • Examine os registros de rastreamento externos para todas as mídias.	☐	☐	☐	☐	☐
9.4.4	A gerência aprova todas as mídias com os dados do titular do cartão que são movidos para fora das instalações (incluindo quando a mídia é distribuída para indivíduos).	• Examine os procedimentos documentados. • Examine os registros de rastreamento de mídia externa. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Os indivíduos que aprovam movimentos de mídia devem ter o nível apropriado de autoridade administrativa para conceder essa aprovação. Entretanto, não é especificamente exigido que tais indivíduos tenham “gerente” como parte de seu cargo.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.4.5	Registros de inventário de todas as mídias eletrônicas com os dados do titular do cartão são mantidos.	• Examine os procedimentos documentados. • Examine os registros do inventário de mídia eletrônica . • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
9.4.5.1	Os inventários de mídia eletrônica com os dados do titular do cartão são realizados pelo menos uma vez a cada 12 meses.	• Examine os procedimentos documentados. • Examine os registros do inventário de mídia eletrônica . • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
9.4.6	Os materiais impressos com os dados do titular do cartão são destruídos quando não são mais necessários para negócios ou razões jurídicas, da seguinte forma: • Os materiais são retalhados, incinerados ou transformados em pó para que os dados do titular do cartão não possam ser reconstruídos. • Os materiais são armazenados em recipientes de armazenamento seguro antes da destruição	• Examine a política de destruição de mídia. • Observe os processos. • Entreviste o pessoal. • Observe os recipientes de armazenamento.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esses requisitos para destruição de mídia quando essa mídia não é mais necessária para negócios ou razões jurídicas são separados e distintos do Requisito 3.2.1 do PCI DSS, que é para excluir com segurança os dados do titular do cartão quando não forem mais necessários de acordo com as políticas de retenção de dados do titular do cartão da entidade.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.4.7	A mídia eletrônica com os dados do titular do cartão é destruída quando não é mais necessária para negócios ou razões jurídicas por meio de um dos seguintes: • A mídia eletrônica é destruída. • Os dados do titular do cartão são tornados irrecuperáveis para que não possam ser reconstruídos.	• Examine a política de destruição de mídia. • Observe o processo de destruição da mídia. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esses requisitos para destruição de mídia quando essa mídia não é mais necessária para negócios ou razões jurídicas são separados e distintos do Requisito 3.2.1 do PCI DSS, que é para excluir com segurança os dados do titular do cartão quando não forem mais necessários de acordo com as políticas de retenção de dados do titular do cartão da entidade.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.5 Dispositivos de ponto de interação (POI) são protegidos contra adulteração e substituição não autorizada.							
9.5.1	Dispositivos POI que capturam dados de cartão de pagamento por meio de interação física direta com o fator de forma do cartão de pagamento são protegidos contra adulteração e substituição não autorizada, incluindo o seguinte: • Manter uma lista de dispositivos POI. • Inspecionar periodicamente os dispositivos POI para procurar adulteração ou substituição não autorizada. • Treinar o pessoal para estar ciente de comportamentos suspeitos e para relatar adulteração ou substituição não autorizada de dispositivos.	• Examine as políticas e procedimentos documentados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Esses requisitos se aplicam a dispositivos POI implantados usados em transações com cartão presente (ou seja, uma forma de cartão de pagamento, como um cartão que é passado, lido por aproximação ou inserido). Estes requisitos não se aplicam a: • Componentes usados apenas para entrada manual da chave PAN. • Dispositivos comerciais de prateleira (COTS) (por exemplo, smartphones ou tablets), que são dispositivos móveis de propriedade do comerciante projetados para distribuição no mercado de massa.						
9.5.1.1	Uma lista atualizada de dispositivos POI é mantida, incluindo: • Fabricação e modelo do dispositivo.. • Localização do dispositivo. • Número de série do dispositivo ou outros métodos de identificação exclusiva.	• Examine a lista de dispositivos POI. • Observe os dispositivos POI e as localizações dos dispositivos. • Entreviste o pessoal.	☐	☐	☐	☐	☐
9.5.1.2	As superfícies do dispositivo POI são inspecionadas periodicamente para detectar adulteração e substituição não autorizada.	• Examine os procedimentos documentados. • Entreviste o pessoal responsável. • Observe os processos de inspeção.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
9.5.1.2.1	A frequência das inspeções periódicas do dispositivo POI e o tipo de inspeções realizadas são definidos na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	• Examine a análise de risco direcionada. • Examine os resultados documentados das inspeções periódicas do dispositivo. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.						
9.5.1.3	O treinamento é fornecido para o pessoal em ambientes de POI estar ciente de tentativa de adulteração ou substituição de dispositivos de POI, e inclui: • Verificar a identidade de terceiros que afirmam ser funcionários de reparos ou manutenção, antes de conceder-lhes acesso para modificar ou solucionar problemas de dispositivos. • Procedimentos para garantir que os dispositivos não sejam instalados, substituídos ou devolvidos sem verificação. • Estar ciente de comportamentos suspeitos em torno de dispositivos. • Relatar comportamento suspeito e indicações de adulteração ou substituição do dispositivo ao pessoal apropriado.	• Revise os materiais de treinamento para o pessoal em ambientes POI. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

Monitorar e Testar as Redes Regularmente

Requisito 10: Registrar e Monitorar Todo o Acesso aos Componentes do Sistema e Dados do Titular do Cartão

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.1 Processos e mecanismos para registrar e monitorar todos os acessos aos componentes do sistema e aos dados do titular do cartão são definidos e entendidos.							
10.1.1	Todas as políticas e processos operacionais identificados no Requisito 10 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
10.1.2	As funções e responsabilidades para a execução de atividades no Requisito 10 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
10.2 Os registros de auditoria são implementados para apoiar a detecção de anomalias e atividades suspeitas, e a análise forense de eventos.							
10.2.1	Os registros de auditoria estão habilitados e ativos para todos os componentes do sistema e dados do titular do cartão.	• Entreviste o administrador do sistema. • Examine as configurações do sistema.	☐	☐	☐	☐	☐
10.2.1.1	Os registros de auditoria capturam todos os acessos individuais do usuário aos dados do titular do cartão.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.2.1.2	Os registros de auditoria capturam todas as ações realizadas por qualquer indivíduo com acesso administrativo, incluindo qualquer uso interativo de aplicativos ou contas do sistema.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.2.1.3	Os registros de auditoria capturam todo o acesso aos registros de auditoria.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.2.1.4	Os registros de auditoria capturam todas as tentativas de acesso lógico inválido.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.2.1.5	Os registros de auditoria capturam todas as mudanças nas credenciais de identificação e autenticação, incluindo, mas não se limitando a: • Criação de novas contas. • Elevação de privilégios. • Todas as mudanças, adições ou exclusões de contas com acesso administrativo.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.2.1.6	Os registros de auditoria capturam o seguinte: • Todas as inicializações de novos registros de auditoria e • Tudo o que estiver iniciando, parando ou pausando os registros de auditoria existentes.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.2.1.7	Os registros de auditoria capturam toda a criação e exclusão de objetos no nível do sistema.	• Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.2.2	Os registros de auditoria registram os seguintes detalhes para cada evento auditável: • Identificação do Usuário. • Tipo de evento. • Data e hora. • Indicação de sucesso e fracasso. • Origem do evento. • Identidade ou nome dos dados afetados, componente do sistema, recurso ou serviço (por exemplo, nome e protocolo).	• Entreviste o pessoal responsável. • Examine as configurações do registro de auditoria. • Examine os dados do registro de auditoria.	☐	☐	☐	☐	☐
10.3 Os registros de auditoria são protegidos contra destruição e modificações não autorizadas.							
10.3.1	O acesso de leitura aos arquivos de registros de auditoria é limitado àqueles com uma necessidade relacionada ao trabalho.	• Entreviste os administradores do sistema • Examine as configurações e privilégios do sistema.	☐	☐	☐	☐	☐
10.3.2	Os arquivos de registros de auditoria são protegidos para evitar modificações por indivíduos.	• Examine as configurações e privilégios do sistema. • Entreviste os administradores do sistema.	☐	☐	☐	☐	☐
10.3.3	Os arquivos de registro de auditoria, incluindo aqueles para tecnologias externas, são imediatamente copiados para um(ns) servidor(es) de registro interno(s) seguro(s) central(is) ou outra mídia de difícil modificação.	• Examine as configurações de backup ou arquivos de registro.	☐	☐	☐	☐	☐
10.3.4	O monitoramento da integridade do arquivo ou mecanismos de detecção de mudança são usados em registros de auditoria para garantir que os dados de registro existentes não possam ser alterados sem gerar alertas.	• Examine as configurações do sistema. • Examine os arquivos monitorados. • Examine os resultados das atividades de monitoramento.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.4 Os registros de auditoria revisados para identificar anomalias ou atividades suspeitas.							
10.4.1	Os seguintes registros de auditoria são revisados pelo menos uma vez ao dia: • Todos os eventos de segurança. • Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD. • Registros de todos os componentes críticos do sistema. • Registros de todos os servidores e componentes do sistema que executam funções de segurança (por exemplo, controles de segurança de rede, sistemas de detecção de intrusão/sistemas de prevenção de intrusão (IDS/IPS), servidores de autenticação).	• Examine as políticas e procedimentos de segurança. • Observe os processos. • Entreviste o pessoal.	☐	☐	☐	☐	☐
10.4.1.1	Mecanismos automatizados são usados para realizar revisões de registro de auditoria.	• Examine os mecanismos de revisão do registro. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
10.4.2	Os registros de todos os outros componentes do sistema (aqueles não especificados no Requisito 10.4.1) são revisados periodicamente.	• Examine as políticas e procedimentos de segurança. • Examine os resultados documentados das revisões de registro. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito é aplicável a todos os outros componentes do sistema dentro do escopo não incluídos no Requisito 10.4.1.						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.4.2.1	A frequência das revisões de registro periódicas para todos os outros componentes do sistema (não definidos no Requisito 10.4.1) é definida na análise de risco alvo da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1	• Examine a análise de risco direcionada. • Examine os resultados documentados das revisões periódicas dos registros. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
10.4.3	Exceções e anomalias identificadas durante o processo de revisão são abordadas.	• Examine as políticas e procedimentos de segurança. • Observe os processos. • Entreviste o pessoal.	☐	☐	☐	☐	☐
10.5 O histórico do registro de auditoria é retido e está disponível para análise.							
10.5.1	Reter o histórico do registro e auditoria por pelo menos 12 meses, com pelo menos os três meses mais recentes imediatamente disponíveis para análise.	• Examine as políticas e procedimentos documentados de retenção de registros de auditoria. • Examine as configurações do histórico do registro de auditoria. • Examine os registros de auditoria. • Entreviste o pessoal. • Observe os processos.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.6 Os mecanismos de sincronização de tempo suportam configurações de tempo consistentes em todos os sistemas.							
10.6.1	Os relógios e a hora do sistema são sincronizados usando a tecnologia de sincronização de tempo.	• Examine os padrões de configuração do sistema.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Manter a tecnologia de sincronização de tempo atualizada inclui gerenciar vulnerabilidades e corrigir a tecnologia de acordo com os Requisitos 6.3.1 e 6.3.3 do PCI DSS.						
10.6.2	Os sistemas são configurados para o tempo correto e consistente da seguinte forma: • Um ou mais servidores de horário designados estão em uso. • Apenas o(s) servidor(es) de horário central(is) designado(s) recebe(m) o horário de fontes externas. • A hora recebida de fontes externas é baseada na Hora Atômica Internacional ou Hora Universal Coordenada (UTC). • Os servidores de horário designados aceitam atualizações de horário apenas de fontes externas específicas aceitas pelo setor. • Onde houver mais de um servidor de horário designado, os servidores de horário fazem par uns com os outros para manter o horário preciso. • Os sistemas internos recebem informações de horário apenas do(s) servidor(es) de horário central(is) designado(s).	• Examine as definições de configuração do sistema para adquirir, distribuir e armazenar a hora correta.	☐	☐	☐	☐	☐
10.6.3	As configurações de sincronização de tempo e os dados são protegidos da seguinte forma: • O acesso aos dados de tempo é restrito apenas ao pessoal com necessidades comerciais. • Quaisquer mudanças nas configurações de tempo em sistemas críticos são registradas, monitoradas e revisadas.	• Examine as configurações do sistema e as configurações e registros de sincronização de tempo. • Observe os processos.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.7 Falhas de sistemas de controle de segurança críticos são detectadas, relatadas e respondidas prontamente.							
10.7.1	***Requisito adicional apenas para prestadores de serviços.***						
10.7.2	Falhas de sistemas de controle de segurança críticos são detectados, alertados e resolvidos prontamente, incluindo, mas não se limitando a falha dos seguintes sistemas de controle de segurança críticos: • Controles de segurança de rede. • IDS/IPS. • Mecanismos de detecção de mudança • Soluções antimalware. • Controles de acesso físico. • Controles de acesso lógico. • Mecanismos de registro de auditoria. • Controles de segmentação (se usados). • Mecanismos de revisão de registro de auditoria. • Ferramentas de teste de segurança automatizadas (se usadas).	• Examine os processos documentados. • Observe os processos de detecção e alerta. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito se aplica a todas as entidades, incluindo prestadores de serviços, e substituirá o Requisito 10.7.1 a partir de 31 de março de 2025. Inclui dois sistemas de controle de segurança críticos adicionais, não incluídos no Requisito 10.7.1. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta* (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
10.7.3	Falhas de quaisquer sistemas de controle de segurança críticos são respondidas imediatamente, incluindo, mas não se limitando a: • Restaurando funções de segurança. • Identificar e documentar a duração (data e hora do início ao fim) da falha de segurança. • Identificar e documentar a(s) causa(s) da falha e documentar a correção necessária. • Identificar e resolver quaisquer problemas de segurança que surgiram durante a falha. • Determinar se outras ações são necessárias como resultado da falha de segurança. • Implementar controles para evitar que a causa da falha ocorra novamente. • Retomar o monitoramento dos controles de segurança.	• Examine os processos documentados. • Entreviste o pessoal. • Examine os registros relacionados a falhas críticas de sistemas de controle de segurança.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito aplica-se apenas quando a entidade avaliada for prestadora de serviços até 31 de março de 2025, após a qual este requisito será aplicável a todas as entidades. *Este é um requisito atual da v3.2.1 que se aplica apenas aos prestadores de serviços. Entretanto, este requisito é uma prática recomendada para todas as outras entidades até 31 de março de 2025, após o qual será exigido e deverá ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito 11: Testar a Segurança de Sistemas e Redes Regularmente

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.1 Processos e mecanismos para testar regularmente a segurança de sistemas e redes são definidos e compreendidos.							
11.1.1	Todas as políticas e processos operacionais identificados no Requisito 11 estão: • Documentadas. • Atualizadas. • Em uso. • De conhecimento de todas as partes afetadas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
11.1.2	As funções e responsabilidades para a execução de atividades no Requisito 11 são documentadas, atribuídas e compreendidas.	• Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.2 Os pontos de acesso wireless são identificados e monitorados, e os pontos de acesso sem fio não autorizados são apresentados.							
11.2.1	Os pontos de acesso wireless autorizados e não autorizados são gerenciados da seguinte forma: • A presença de pontos de acesso wireless (Wi-Fi) é testada. • Todos os pontos de acesso wireless autorizados e não autorizados são detectados e identificados. • O teste, a detecção e a identificação ocorrem pelo menos uma vez a cada três meses. • Se o monitoramento automatizado for usado, o pessoal será notificado por meio de alertas gerados.	• Examine as políticas e os procedimentos. • Examine a(s) metodologia(s) em uso e a documentação resultante. • Entreviste o pessoal. • Examine os resultados da avaliação wireless. • Examine as definições de configuração.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O requisito se aplica mesmo quando existe uma política que proíbe o uso de tecnologia wireless. Os métodos usados para atender a esse requisito devem ser suficientes para detectar e identificar dispositivos autorizados e não autorizados, incluindo dispositivos não autorizados conectados a dispositivos que são autorizados.						
11.2.2	Um inventário de pontos de acesso wireless autorizados é mantido, incluindo uma justificativa comercial documentada.	• Examine a documentação.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3 Vulnerabilidades externas e internas são regularmente identificadas, priorizadas e tratadas.							
11.3.1	As varreduras de vulnerabilidade interna são realizadas da seguinte forma: • Pelo menos uma vez a cada três meses. • Vulnerabilidades que são ou de alto risco ou críticas (de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) são resolvidas. • Novas varreduras são realizadas para confirmar que todas as vulnerabilidades críticas e de alto risco, (conforme observado acima) foram resolvidas • A ferramenta de varredura é mantida atualizada com as informações mais recentes sobre vulnerabilidades. • As varreduras são realizadas por pessoal qualificado e existe independência organizacional do testador	• Examine os resultados do relatório de varredura interna. • Examine as configurações da ferramenta de varredura. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Não é necessário usar um QSA ou ASV para realizar varreduras de vulnerabilidade interna. Varreduras de vulnerabilidade interna podem ser realizadas por equipe interna qualificada que é razoavelmente independente do(s) componente(s) do sistema que está sendo varrido (por exemplo, um administrador de rede não deve ser responsável pela varredura da rede), ou uma entidade pode escolher ter vulnerabilidade interna varreduras realizadas por uma empresa especializada em varredura de vulnerabilidades.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3.1.1	Todas as outras vulnerabilidades aplicáveis (aquelas não classificadas como vulnerabilidades de alto risco ou crítica de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) são gerenciadas da seguinte forma: • Abordado com base no risco definido na análise de risco alvo da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1. • Novas varreduras são realizadas conforme necessário.	• Examine a análise de risco direcionada. • Entreviste o pessoal responsável. • Examine os resultados do relatório de varredura interna ou outra documentação.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O prazo para abordar vulnerabilidades de risco mais baixo está sujeito aos resultados de uma análise de risco de acordo com o Requisito 12.3.1 que inclui a identificação (mínima) dos ativos sendo protegidos, ameaças e probabilidade e/ou impacto de uma ameaça sendo realizada. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3.1.2	Varreduras de vulnerabilidade interna são realizadas por meio de varredura autenticada da seguinte forma:						
	• Os sistemas que não aceitam credenciais para varredura autenticada são documentados.	• Examine a documentação. • Examine as configurações da ferramenta de varredura. • Examine os resultados do relatório de varredura. • Entreviste o pessoal. • Examine as contas usadas para varredura autenticada.	☐	☐	☐	☐	☐
	• Privilégios suficientes são usados para os sistemas que aceitam credenciais para varredura.		☐	☐	☐	☐	☐
	• Se as contas usadas para varredura autenticada puderem ser usadas para login interativo, elas serão gerenciadas de acordo com o Requisito 8.2.2.		☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	As ferramentas de varreduras autenticadas podem ser baseadas em host ou em rede. Privilégios ”suficientes são aqueles necessários para acessar os recursos do sistema de forma que uma varredura completa possa ser realizada para detectar vulnerabilidades conhecidas. Este requisito não se aplica a componentes do sistema que não podem aceitar credenciais para varredura. Exemplos de sistemas que podem não aceitar credenciais para varredura incluem alguns dispositivos de rede e segurança, mainframes e contêineres *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3.1.3	As varreduras de vulnerabilidades internas são executadas após qualquer mudança significativa da seguinte forma: • Vulnerabilidades que são ou de alto risco ou críticas (de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) são resolvidas. • Novas varreduras são realizadas conforme necessário. • As varreduras são realizadas por pessoal qualificado e existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	• Examine a documentação de controle de mudanças. • Entreviste o pessoal. • Examine a varredura interna e o relatório de nova varredura conforme aplicável. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade A varredura de vulnerabilidade interna autenticada de acordo com o Requisito 11.3.1.2 não é necessária para varreduras realizadas após mudanças significativas.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3.2	As varreduras de vulnerabilidade externa são realizadas da seguinte forma: • Pelo menos uma vez a cada três meses. • Por um Fornecedor de Varredura Aprovado do PCI SSC (ASV). • As vulnerabilidades foram resolvidas e os requisitos do *Guia do Programa ASV* para uma varredura de aprovação foram atendidos. • As novas varreduras são realizadas conforme necessário para confirmar que as vulnerabilidades foram resolvidas de acordo com os requisitos do *Guia do Programa ASV* para uma varredura de aprovação.	• Examine os relatórios de varredura ASV.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Para avaliação inicial com o PCI DSS em relação a este requisito, não é necessário que quatro varreduras aprovadas sejam concluídas dentro de 12 meses se o assessor verificar: 1) o resultado da varredura mais recente foi uma varredura de aprovação, 2) a entidade documentou políticas e procedimentos que exigem varredura pelo menos uma vez a cada três meses e 3) as vulnerabilidades observadas nos resultados da varredura foram corrigidas conforme mostrado em uma(umas) nova(s) varredura(s). No entanto, nos anos subsequentes após a avaliação inicial do PCI DSS, as varreduras devem ter ocorrido pelo menos a cada três meses. As ferramentas de varredura ASV podem varrer uma vasta gama de tipos e topologias de rede. Quaisquer especificações sobre o ambiente de destino (por exemplo, balanceadores de carga, prestadores terceirizados, ISPs, configurações específicas, protocolos em uso, interferência de varredura) devem ser resolvidas entre o ASV e o cliente de varredura. Consulte o *Guia do Programa ASV* publicado no site PCI SSC para verificar as responsabilidades do cliente, a preparação da varredura, etc.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.3.2.1	As varreduras de vulnerabilidades externas são executadas após qualquer mudança significativa da seguinte forma: • Vulnerabilidades com pontuação de 4.0 ou superior pelo CVSS são resolvidas. • Novas varreduras são realizadas conforme necessário. • As varreduras são realizadas por pessoal qualificado e existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	• Examine a documentação de controle de mudanças. • Entreviste o pessoal. • Examine a varredura externa e, conforme aplicável, os relatórios de nova varredura.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.4 Testes de penetração externos e internos são realizados regularmente e vulnerabilidades exploráveis e fragilidades de segurança são corrigidas.							
11.4.1	Uma metodologia de teste de penetração é definida, documentada e implementada pela entidade e inclui: • Abordagens de teste de penetração aceitas pela indústria. • Cobertura para todo o perímetro CDE e sistemas críticos. • Testando dentro e fora da rede. • Teste para validar qualquer segmentação e controles de redução de escopo. • Teste de penetração na camada de aplicativo para identificar, no mínimo, as vulnerabilidades listadas no Requisito 6.2.4. • Testes de penetração na camada de rede que abrangem todos os componentes que suportam funções de rede, bem como sistemas operacionais. • Revisão e consideração de ameaças e vulnerabilidades experimentadas nos últimos 12 meses • Abordagem documentada para avaliar e abordar o risco representado por vulnerabilidades exploráveis e pontos fracos de segurança encontrados durante o teste de penetração. • Retenção dos resultados dos testes de penetração e resultados das atividades de remediação por pelo menos 12 meses.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Testar de dentro da rede (ou “teste de penetração interna”) significa testar de dentro do CDE e no CDE de redes internas confiáveis e não confiáveis. Teste de fora da rede (ou teste de penetração “externo” significa testar o perímetro externo exposto de redes confiáveis e sistemas críticos conectados ou acessíveis a infraestruturas de rede pública.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.4.2	O teste de penetração interna é realizado: • De acordo com a metodologia definida pela entidade • Pelo menos uma vez a cada 12 meses. • Depois de qualquer infraestrutura significativa ou atualização ou mudança de aplicativo • Por um recurso interno qualificado ou um terceiro externo qualificado • Existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	• Examine o escopo do trabalho. • Examine os resultados do teste de penetração externa mais recente. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
11.4.3	O teste de penetração externa é realizado: • De acordo com a metodologia definida pela entidade • Pelo menos uma vez a cada 12 meses. • Depois de qualquer infraestrutura significativa ou atualização ou mudança de aplicativo • Por um recurso interno qualificado ou um terceiro externo qualificado • Existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	• Examine o escopo do trabalho. • Examine os resultados do teste de penetração externa mais recente. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
11.4.4	Vulnerabilidades exploráveis e fragilidades de segurança encontradas durante o teste de penetração são corrigidas da seguinte forma: • De acordo com a avaliação da entidade do risco representado pelo problema de segurança, conforme definido no Requisito 6.3.1. • O teste de penetração é repetido para verificar as correções.	• Examine os resultados dos testes de penetração.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.4.5	Se a segmentação for usada para isolar o CDE de outras redes, os testes de penetração são realizados nos controles de segmentação da seguinte forma: • Pelo menos uma vez a cada 12 meses e após quaisquer alterações nos controles/métodos de segmentação • Abrangendo todos os controles/métodos de segmentação em uso. • De acordo com a metodologia de teste de penetração definida pela entidade. • Confirmar se os controles/métodos de segmentação são operacionais e eficazes e isolar o CDE de todos os sistemas fora do escopo. • Confirmação da eficácia de qualquer uso de isolamento para sistemas separados com diferentes níveis de segurança (consulte o Requisito 2.2.3). • Executado por um recurso interno qualificado ou um terceiro externo qualificado. • Existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	• Examine os controles de segmentação. • Revise a metodologia de teste de penetração. • Examine os resultados do teste de penetração mais recente. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
11.4.6	***Requisito adicional apenas para prestadores de serviços.***						
11.4.7	***Requisito adicional apenas para prestadores de serviços multilocatários.***						

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.5 Intrusões de rede e mudanças inesperadas de arquivos são detectadas e respondidas.							
11.5.1	Técnicas de detecção de intrusão e/ou prevenção de intrusão são usadas para detectar e/ou prevenir intrusões na rede da seguinte forma: • Todo o tráfego é monitorado no perímetro do CDE • Todo o tráfego é monitorado em pontos críticos do CDE. • O pessoal é alertado sobre suspeitas de comprometimento. • Todos os mecanismos de detecção e prevenção de intrusão, linhas de base e assinaturas são mantidos atualizados.	• Examine as configurações do sistema e os diagramas de rede. • Examine as configurações do sistema. • Entreviste o pessoal responsável. • Examine a documentação do fornecedor.	☐	☐	☐	☐	☐
11.5.1.1	***Requisito adicional apenas para prestadores de serviços***						
11.5.2	Um mecanismo de detecção de mudança (por exemplo, ferramentas de monitoramento de integridade de arquivo) é implantado da seguinte forma: • Para alertar o pessoal sobre modificações não autorizadas (incluindo mudanças, adições e exclusões) de arquivos críticos. • Para realizar comparações críticas de arquivos pelo menos uma vez por semana.	• Examine as configurações do sistema para o mecanismo de detecção de mudanças. • Examine os arquivos monitorados. • Examine os resultados das atividades de monitoramento.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Para fins de detecção de mudanças, os arquivos críticos geralmente são aqueles que não mudam regularmente, mas a modificação dos quais pode indicar comprometimento do sistema ou risco de comprometimento. Mecanismos de detecção de mudanças, como produtos de monitoramento de integridade de arquivos, geralmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
11.6 Mudanças não autorizadas nas páginas de pagamento são detectadas e respondidas.							
11.6.1	Um mecanismo de detecção de mudanças e adulterações é implantado da seguinte forma:						
	• Para alertar o pessoal sobre modificações não autorizadas (incluindo indicadores de comprometimento, alterações, adições e exclusões) nos cabeçalhos que impactam a segurança do HTTP e no conteúdo de scripts das páginas de pagamento recebidas pelo navegador do consumidor.	• Examine as configurações do sistema e as configurações do mecanismo. • Examine as páginas de pagamento monitoradas. • Examine os resultados das atividades de monitoramento. • Examine as definições de configuração do mecanismo. • Examine as definições de configuração. • Entreviste o pessoal responsável. • Se aplicável, examine a análise de risco direcionada.	☐	☐	☐	☐	☐
	• O mecanismo é configurado para avaliar os cabeçalhos HTTP recebidos e as páginas de pagamento.		☐	☐	☐	☐	☐
	• As funções do mecanismo são realizadas da seguinte forma: – Pelo menos uma vez por semana **OU** – Periodicamente (na frequência definida na análise de risco alvo da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1). *(continuação)*		☐	☐	☐	☐	☐

Requisito do PCI DSS	Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
		Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
Observações de Aplicabilidade Este requisito também se aplica a entidades com páginas da Web que incluam uma página/formulário de pagamento incorporado de um TPSP/processador de pagamento (por exemplo, um ou mais frames ou iframes inline). Este requisito não se aplica a uma entidade para scripts em uma página/formulário de pagamento incorporado de um TPSP/processador de pagamento (por exemplo, um ou mais iframes), onde a entidade inclui uma página/formulário de pagamento de um TPSP/processador de pagamento em sua página da web. Os scripts na página/formulário de pagamento incorporado do TPSP/processador de pagamento são de responsabilidade do TPSP/processador de pagamento para serem gerenciados de acordo com este requisito. A intenção deste requisito não é que uma entidade instale software nos sistemas ou navegadores de seus consumidores, mas sim que a entidade use técnicas como as descritas em Exemplos na coluna Diretrizes do PCI DSS para prevenir e detectar atividades de script inesperadas. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Manter uma Política de Segurança da Informação

Requisito 12: Apoiar a Segurança da Informação com Políticas e Programas Organizacionais

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.1 Uma política abrangente de segurança da informação que governa e fornece orientação para a proteção dos ativos de informação da entidade é conhecida e atual.							
12.1.1	Uma política geral de segurança da informação é: • Estabelecida. • Publicada. • Mantidos • Divulgada para todo o pessoal relevante, bem como para fornecedores e parceiros de negócios relevantes.	• Examine a política de segurança da informação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
12.1.2	A política de segurança da informação está: • Revisada pelo menos uma vez a cada 12 meses. • Atualizada conforme necessário para refletir mudanças nos objetivos de negócios ou riscos ao meio ambiente.	• Examine a política de segurança da informação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
12.1.3	A política de segurança define claramente as funções e responsabilidades de segurança da informação para todo o pessoal, e todo o pessoal está ciente e reconhece suas responsabilidades pela segurança da informação.	• Examine a política de segurança da informação. • Entreviste o pessoal responsável. • Examine as evidências documentadas.	☐	☐	☐	☐	☐
12.1.4	A responsabilidade pela segurança da informação é formalmente atribuída a um diretor de segurança da informação ou outro membro da gerência executiva com conhecimento em segurança da informação.	• Examine a política de segurança da informação.	☐	☐	☐	☐	☐

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.2 Políticas de uso aceitável para tecnologias de usuário final são definidas e implementadas.							
12.2.1	Políticas de uso aceitável para tecnologias de usuário final são documentadas e implementadas, incluindo: • Aprovação explícita por partes autorizadas. • Usos aceitáveis da tecnologia. • Lista de produtos aprovados pela empresa para uso dos funcionários, incluindo hardware e software.	• Examine as políticas de uso aceitável. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Exemplos de tecnologias de usuário final para as quais políticas de uso aceitáveis são esperadas incluem, mas não estão limitadas a, acesso remoto e tecnologias wireless, laptops, tablets, telefones celulares e mídia eletrônica removível, uso de e-mail e uso da Internet.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.3 Os riscos para o ambiente de dados do titular do cartão são formalmente identificados, avaliados e gerenciados.							
12.3.1	Para cada requisito PCI DSS que especifica a conclusão de uma análise de risco direcionada, tal análise é documentada e inclui: • Identificação dos bens protegidos. • Identificação das ameaças contra as quais o requisito está protegendo. • Identificação de fatores que contribuem para a probabilidade e/ou impacto de uma ameaça se concretizar. • Análise resultante que determina e inclui a justificativa para como a frequência ou processos definidos pela entidade para atender ao requisito minimiza a probabilidade e/ou o impacto de a ameaça ser realizada. • Revisão de cada análise de risco direcionada pelo menos uma vez a cada 12 meses para determinar se os resultados ainda são válidos ou se uma análise de risco atualizada é necessária • Execução de análises de risco atualizadas quando necessário, conforme determinado pela revisão anual.	• Examine as políticas e procedimentos documentados.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
12.3.2	***Este requisito é específico da abordagem personalizada e não se aplica a entidades que preencham um questionário de autoavaliação.***						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.3.3	Conjuntos de cifras criptográfica e protocolos em uso são documentados e revisados pelo menos uma vez a cada 12 meses, incluindo pelo menos o seguinte: • Um inventário atualizado de todos os conjuntos de cifras criptográficas e protocolos em uso, incluindo a finalidade e o local de uso. • Monitoramento ativo das tendências da indústria em relação à viabilidade contínua de todos os pacotes e protocolos de criptografia criptográfica em uso. • Documentação de um plano para responder às mudanças previstas nas vulnerabilidades criptográficas.	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade O requisito se aplica a todos os conjuntos de cifras criptográficas e protocolos usados para atender aos requisitos do PCI DSS, incluindo, mas não se limitando a, aqueles usados para tornar o PAN ilegível no armazenamento e transmissão, para proteger senhas e como parte da autenticação de acesso. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.3.4	As tecnologias de hardware e software em uso são revisadas pelo menos uma vez a cada 12 meses, incluindo pelo menos o seguinte: • Análise de que as tecnologias continuam recebendo correções de segurança dos fornecedores prontamente. • Análise de que as tecnologias continuam a oferecer suporte (e não impedem) a conformidade com PCI DSS da entidade. • Documentação de quaisquer anúncios ou tendências do setor relacionados a uma tecnologia, como quando um fornecedor anuncia planos de "fim de vida" para uma tecnologia. • Documentação de um plano, aprovado pela alta administração, para remediar tecnologias desatualizadas, incluindo aquelas para as quais os fornecedores anunciaram planos de "fim de vida".	• Examine a documentação. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
12.4 A conformidade com PCI DSS é gerenciada.							
12.4.1	***Requisito adicional apenas para prestadores de serviços.***						
12.4.2	***Requisito adicional apenas para prestadores de serviços.***						
12.4.2.1	***Requisito adicional apenas para prestadores de serviços.***						
12.5 O escopo do PCI DSS é documentado e validado.							
12.5.1	Um inventário dos componentes do sistema que estão no escopo do PCI DSS, incluindo uma descrição de função/uso, é mantido e atualizado.	• Examine o inventário. • Entreviste o pessoal.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.5.2	O escopo do PCI DSS é documentado e confirmado pela entidade pelo menos uma vez a cada 12 meses e mediante mudança significativa no ambiente dentro do escopo.	• Examine os resultados documentados das revisões do escopo. • Entreviste o pessoal.	☐	☐	☐	☐	☐
	No mínimo, a validação do escopo inclui:						
	• Identificar todos os fluxos de dados para os vários estágios de pagamento (por exemplo autorização, liquidação de captura, estornos e reembolsos) e canais de aceitação (por exemplo, cartão presente, cartão ausente e comércio eletrônico).	• Examine os resultados documentados das revisões do escopo.	☐	☐	☐	☐	☐
	• Atualizar todos os diagramas de fluxo de dados por requisito 1.2.4.		☐	☐	☐	☐	☐
	• Identificar todos os locais onde os dados da conta são armazenados, processados e transmitidos, incluindo, mas não se limitando a: 1) quaisquer locais fora do CDE atualmente definido, 2) aplicativos que processam CHD, 3) transmissões entre sistemas e redes e 4) backups de arquivos.		☐	☐	☐	☐	☐
	• Identificar todos os componentes do sistema no CDE, conectados ao CDE ou que possam impactar a segurança do CDE.		☐	☐	☐	☐	☐
	• Identificar todos os controles de segmentação em uso e os ambientes dos quais o CDE é segmentado, incluindo a justificativa para ambientes que estão fora do escopo.		☐	☐	☐	☐	☐
	• Identificar todas as conexões de entidades de terceiros com acesso ao CDE. *(continuação)*		☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
	• Confirmar se todos os fluxos de dados identificados, dados da conta, componentes do sistema, controles de segmentação e conexões de terceiros com acesso ao CDE estão incluídos no escopo.		☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Esta confirmação anual do escopo do PCI DSS é uma atividade que se espera que seja realizada pela entidade sob avaliação e não é a mesma, nem se destina a ser substituída pela confirmação do escopo realizada pelo assessor da entidade durante a avaliação anual.						
12.5.2.1	***Requisito adicional apenas para prestadores de serviços.***						
12.5.3	***Requisito adicional apenas para prestadores de serviços.***						
12.6 A formação de uma conscientização sobre segurança é uma atividade contínua.							
12.6.1	Um programa formal de conscientização de segurança é implementado para conscientizar todo o pessoal sobre a política e procedimentos de segurança da informação da entidade e sua função na proteção dos dados do titular do cartão.	• Examine o programa de conscientização de segurança.	☐	☐	☐	☐	☐
12.6.2	O programa de conscientização de segurança é: • Revisado pelo menos uma vez a cada 12 meses, e • Atualizado conforme necessário para lidar com quaisquer novas ameaças e vulnerabilidades que possam afetar a segurança dos dados do titular do cartão e/ou dos dados de autenticação confidenciais da entidade ou as informações fornecidas ao pessoal sobre sua função na proteção dos dados do titular do cartão. *(continuação)*	• Examine o conteúdo do programa de conscientização de segurança. • Examine as evidências de revisões. • Entreviste o pessoal.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ (Marque uma resposta para cada requisito)				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
12.6.3	O pessoal recebe treinamento de conscientização de segurança da seguinte forma: • No momento da contratação e pelo menos uma vez a cada 12 meses. • Vários métodos de comunicação são usados. • O pessoal reconhece, pelo menos uma vez a cada 12 meses, que leu e compreendeu a política e os procedimentos de segurança da informação.	• Examine os registros do programa de conscientização de segurança. • Entreviste o pessoal aplicável. • Examine os materiais do programa de conscientização de segurança. • Examine os reconhecimentos de pessoal.	☐	☐	☐	☐	☐
12.6.3.1	O treinamento de conscientização sobre segurança inclui a conscientização de ameaças e vulnerabilidades que podem impactar a segurança dos dados do titular do cartão e/ou dos dados de autenticação confidenciais, incluindo, mas não se limitando a: • Phishing e ataques relacionados. • Engenharia social.	• Examine o conteúdo do treinamento de conscientização de segurança.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Consulte o Requisito 5.4.1 no PCI DSS para obter orientação sobre a diferença entre os controles técnicos e automatizados para detectar e proteger os usuários de ataques de phishing e este requisito para fornecer aos usuários treinamento de conscientização de segurança sobre phishing e engenharia social. Esses são dois requisitos separados e distintos, e um não é atendido pela implementação dos controles exigidos pelo outro. *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.6.3.2	O treinamento de conscientização de segurança inclui a conscientização sobre o uso aceitável de tecnologias de usuário final de acordo com o Requisito 12.2.1.	• Examine o conteúdo do treinamento de conscientização de segurança.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.						
12.7 O pessoal é examinado para reduzir os riscos de ameaças internas.							
12.7.1	O pessoal potencial que terá acesso ao CDE é examinado, dentro das restrições das leis locais, antes da contratação para minimizar o risco de ataques de fontes internas.	• Entreviste o pessoal de gestão do departamento de Recursos Humanos responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	Para o pessoal potencial a ser contratado para cargos como caixa de loja, que só tem acesso a um número de cartão por vez ao facilitar uma transação, esse requisito é apenas uma recomendação.						
12.8 O risco aos ativos de informação associados aos relacionamentos com o prestador de serviços terceirizado (TPSP) é gerenciado.							
12.8.1	Uma lista de todos os prestadores de serviços terceirizados (TPSPs) com os quais os dados da conta são compartilhados ou que podem afetar a segurança dos dados da conta é mantida, incluindo uma descrição para cada um dos serviços prestados.	• Examine as políticas e os procedimentos. • Examine a lista de TPSPs.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade						
	O uso de um TPSP compatível com PCI DSS não torna uma entidade compatível com PCI DSS, nem remove a responsabilidade da entidade por sua própria conformidade com o PCI DSS.						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.8.2	Os acordos por escrito com TPSPs são mantidos da seguinte forma: • Acordos por escrito são mantidos com todos os TPSPs com os quais os dados da conta são compartilhados ou que possam afetar a segurança do CDE. • Acordos escritos incluem reconhecimentos dos TPSPs de que são responsáveis pela segurança dos dados da conta que os TPSPs possuem ou armazenam, processam ou transmitem em nome da entidade, ou na medida em que os TPSPs possam impactar a segurança dos dados do titular do cartão e/ou dos dados de autenticação confidenciais da entidade.	• Examine as políticas e os procedimentos. • Examine os acordos escritos com os TPSPs.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade A redação exata de um acordo dependerá dos detalhes do serviço prestado e das responsabilidades atribuídas a cada uma das partes. O acordo não precisa incluir a redação exata fornecida neste requisito. A confirmação por escrito do TPSP é uma confirmação que afirma que o TPSP é responsável pela segurança dos dados da conta que pode armazenar, processar ou transmitir em nome do cliente ou na medida em que o TPSP possa impactar a segurança dos dados do titular do cartão de um cliente e/ ou dados de autenticação confidenciais. A evidência de que um TPSP está atendendo aos requisitos do PCI DSS não é o mesmo que um reconhecimento escrito especificado neste requisito. Por exemplo, um Atestado de Conformidade (AOC) do PCI DSS, uma declaração no site de uma empresa, uma declaração de política, uma matriz de responsabilidade ou outra evidência não incluída em um acordo por escrito não é um reconhecimento por escrito.						
12.8.3	Um processo estabelecido é implementado para envolver os TPSPs, incluindo a due dilligence antes do envolvimento.	• Examine as políticas e os procedimentos. • Examine a evidência. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.8.4	Um programa é implementado para monitorar o status de conformidade do PCI DSS dos TPSPs pelo menos uma vez a cada 12 meses.	• Examine as políticas e os procedimentos. • Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Quando uma entidade tem um contrato com um TPSP para atender aos requisitos do PCI DSS em nome da entidade (por exemplo, por meio de um serviço de firewall), a entidade deve trabalhar com o TPSP para garantir que os requisitos aplicáveis do PCI DSS sejam atendidos. Se o TPSP não atender a esses requisitos aplicáveis do PCI DSS, esses requisitos também "não estão implementados" para a entidade.						
12.8.5	São mantidas informações sobre quais requisitos do PCI DSS são gerenciados por cada TPSP, que são gerenciados pela entidade e quaisquer que sejam compartilhados entre o TPSP e a entidade.	• Examine as políticas e os procedimentos. • Examine a documentação. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
12.9 Os prestadores de serviços terceirizados (TPSPs) oferecem suporte à conformidade com o PCI DSS de seus clientes.							
12.9.1	***Requisito adicional apenas para prestadores de serviços.***						
12.9.2	***Requisito adicional apenas para prestadores de serviços.***						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.10 Incidentes de segurança suspeitos e confirmados que poderiam impactar o CDE são respondidos imediatamente.							
12.10.1	Um plano de resposta a incidentes existe e está pronto para ser ativado no caso de um incidente de segurança suspeito ou confirmado. O plano inclui, mas não está limitado a: • Funções, responsabilidades e estratégias de comunicação e contato no caso de um incidente de segurança suspeito ou confirmado, incluindo notificação de bandeiras de pagamento e adquirentes, no mínimo. • Procedimentos de resposta a incidentes com atividades específicas de contenção e mitigação para diferentes tipos de incidentes. • Procedimentos de recuperação e continuidade de negócios • Processos de backup de dados. • Análise de requisitos jurídicos para comprometimento de relatórios. • Cobertura e respostas de todos os componentes críticos do sistema. • Referência ou inclusão de procedimentos de resposta a incidentes das bandeiras de pagamento.	• Examine o plano de resposta a incidentes. • Entreviste o pessoal. • Examine a documentação de incidentes relatados anteriormente.	☐	☐	☐	☐	☐
12.10.2	Pelo menos uma vez a cada 12 meses, o plano de resposta a incidentes de segurança é: • Revisado e o conteúdo é atualizado conforme necessário. • Testado, incluindo todos os elementos listados no Requisito 12.10.1.	• Entreviste o pessoal. • Examine a documentação.	☐	☐	☐	☐	☐
12.10.3	Pessoal específico é designado para estar disponível 24 horas por dia, 7 dias por semana, para responder a incidentes de segurança suspeitos ou confirmados.	• Entreviste o pessoal responsável. • Examine a documentação.	☐	☐	☐	☐	☐

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.10.4	O pessoal responsável por responder a incidentes de segurança suspeitos e confirmados é adequado e periodicamente treinado em suas responsabilidades de resposta a incidentes.	• Entreviste o pessoal de resposta a incidentes. • Examine a documentação do treinamento.	☐	☐	☐	☐	☐
12.10.4.1	A frequência do treinamento periódico para o pessoal de resposta a incidentes é definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	• Examine a análise de risco direcionada.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						
12.10.5	O plano de resposta a incidentes de segurança inclui monitorar e responder a alertas de sistemas de monitoramento de segurança, incluindo, mas não se limitando a: • Sistemas de detecção e prevenção de intrusão. • Controles de segurança de rede. • Mecanismos de detecção de alterações para arquivos críticos. • O mecanismo de detecção de alterações e adulterações para páginas de pagamento. *Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes.* • Detecção de pontos de acesso wireless *não autorizados.*	• Examine a documentação. • Observe os processos de resposta a incidentes.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *O marcador acima (para monitorar e responder a alertas de um mecanismo de detecção de alteração e violação para páginas de pagamento) é uma prática recomendada até 31 de março de 2025, após o qual será exigido como parte do Requisito 12.10.5 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
12.10.6	O plano de resposta a incidentes de segurança é modificado e evoluído de acordo com as lições aprendidas e para incorporar os desenvolvimentos da indústria.	• Examine as políticas e os procedimentos. • Examine o plano de resposta a incidentes de segurança. • Entreviste o pessoal responsável.	☐	☐	☐	☐	☐
12.10.7	Os procedimentos de resposta a incidentes estão em vigor, para serem iniciados após a detecção de PAN armazenado em qualquer lugar que não seja esperado, e incluem: • Determinar o que fazer se o PAN for descoberto fora do CDE, incluindo sua recuperação, exclusão segura e/ou migração para o CDE definido atualmente, conforme aplicável. • Identificar se os dados de autenticação confidenciais são armazenados com o PAN. • Determinar a origem dos dados da conta e como eles foram parar onde não eram esperados. • Corrigindo vazamentos de dados ou lacunas de processo que resultaram nos dados da conta onde não eram esperados.	• Examine os procedimentos documentados de resposta a incidentes. • Entreviste o pessoal. • Examine os registros das ações de resposta.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade *Este requisito é uma prática recomendada até 31 de março de 2025, após o qual será exigido e deve ser totalmente considerado durante uma avaliação do PCI DSS.*						

Apêndice A: Requisitos Adicionais do PCI DSS

Apêndice A1: Requisitos Adicionais do PCI DSS para Prestadores de Serviços Multilocatários

Este Apêndice não é usado para avaliações de comerciantes.

Apêndice A2: Requisitos Adicionais do PCI DSS para Entidades que usam SSL/TLS Antigo para Conexões de Terminal POS POI com Cartão Presente

Requisito do PCI DSS		Teste Esperado	Resposta♦ *(Marque uma resposta para cada requisito)*				
			Implementado	Implementado com CCW	Não Aplicável	Não Testado	Não Implementado
A2.1 Terminais POI usando SSL e/ou TLS inicial não são suscetíveis a explorações de SSL/TLS conhecidos.							
A2.1.1	Quando os terminais POS POI no estabelecimento ou local de aceitação de pagamento usam SSL e/ou TLS inicial, a entidade confirma que os dispositivos não são suscetíveis a quaisquer explorações conhecidas para esses protocolos.	• Examine a documentação (por exemplo, documentação do fornecedor, detalhes de configuração de sistema/rede) que verifica se os dispositivos não são suscetíveis a quaisquer explorações conhecidas de SSL/TLS anterior.	☐	☐	☐	☐	☐
	Observações de Aplicabilidade Este requisito destina-se a ser aplicado à entidade com o terminal POS POI, como um comerciante. Este requisito não se destina a prestadores de serviço que atuam como ponto de terminação ou conexão para esses terminais POS POI. Os requisitos A2.1.2 e A2.1.3 aplicam-se aos prestadores de serviços PDI POS. A permissão para terminais POS POI que não são atualmente suscetíveis a explorações é baseada nos riscos atualmente conhecidos. Se forem introduzidos novos exploradores aos quais os terminais POS POI são suscetíveis, os terminais POS POI precisarão ser atualizados imediatamente.						
A2.1.2	***Requisito adicional apenas para prestadores de serviços.***						
A2.1.3	***Requisito adicional apenas para prestadores de serviços.***						

♦ *Consulte a seção "Respostas dos Requisitos" (página vi) para obter informações sobre essas opções de resposta.*

Apêndice A3: Validação Complementar de Entidades Designadas (DESV)

Este Apêndice se aplica apenas a entidades designadas por uma(s) bandeira(s) de pagamento ou adquirente como requerendo validação adicional dos requisitos existentes do PCI DSS. As entidades obrigadas a validar este Apêndice devem usar o Modelo de Relatório Complementar do DESV e o Atestado de Conformidade Complementar para relatórios e consultar a bandeira de pagamento e/ou adquirente aplicável para procedimentos de envio.

Apêndice B: Planilha de Controles de Compensação

Este Apêndice deve ser preenchido para definir controles de compensação para qualquer requisito em que Implementado com CCW foi selecionado.

Observação: *Somente entidades que tenham uma restrição tecnológica ou comercial legítima e documentada podem considerar o uso de controles compensatórios para alcançar a conformidade.*

Consulte os Apêndices B e C no PCI DSS para obter informações sobre controles de compensação e orientações sobre como preencher esta planilha.

Número e Definição do Requisito:

	Informações Requeridas	Explicação
1. Limitações	Documente as restrições técnicas ou comerciais legítimas que impedem a conformidade com o requisito original.	
2. Definição de Controles de Compensação	Defina os controles compensatórios: explique como eles abordam os objetivos do controle original e o risco aumentado, se houver.	
3. Objetivo	Defina o objetivo do controle original.	
	Identifique o objetivo alcançado pelo controle de compensação. ***Observação:*** *Isso pode ser, mas não necessariamente, o Objetivo de Abordagem Personalizada declarado listado para este requisito no PCI DSS.*	
4. Risco Identificado	Identifique qualquer risco adicional representado pela falta do controle original.	
5. Validação dos Controles de Compensação	Defina como os controles de compensação foram validados e testados.	
6. Manutenção	Defina o(s) processo(s) e controles implementados para manter os controles de compensação.	

Apêndice C: Explicação dos Requisitos Observados como Não Aplicáveis

Este Apêndice deve ser preenchido para cada requisito em que Não Aplicável foi selecionado.

Requisito	Motivo pelo qual o Requisito é Não Aplicável
Exemplo:	
Requisito 3.5.1	*Os dados da conta nunca são armazenados eletronicamente*

Apêndice D: Explicação dos Requisitos Observados como Não Testados

Este Apêndice deve ser preenchido para cada requisito em que Não Testado foi selecionado.

Requisito	Descrição do(s) Requisito(s) Não Testado(s)	Descreva por que o(s) Requisito(s) foi(foram) Excluído(s) da Avaliação
Exemplos:		
Requisito 10	*Nenhum requisito do Requisito 10 foi testado.*	*Esta avaliação cobre apenas os requisitos do Marco 1 da Abordagem Priorizada.*
Requisitos 1-8, 10-12	*Apenas o Requisito 9 foi revisado para esta avaliação. Todos os outros requisitos foram excluídos.*	*A empresa é uma provedora de hospedagem física (CO-LO), e apenas controles de segurança física foram considerados para esta avaliação.*

Seção 3: Detalhes da Validação e Atestado

Parte 3. Validação do PCI DSS

Este AOC é baseado nos resultados observados no SAQ D (Seção 2), datado (Data de conclusão da autoavaliação *DD-MM-AAAA*).

Indique abaixo se uma avaliação completa ou parcial do PCI DSS foi concluída:

☐ **Completa –** Todos os requisitos foram avaliados e, portanto, nenhum requisito foi marcado como Não Testado no SAQ.

☐ **Parcial –** Um ou mais requisitos não foram avaliados e, portanto, foram marcados como Não Testado no SAQ. Algum requisito não avaliado foi indicado como Não Testado na Parte 2g acima

Com base nos resultados documentados no SAQ D mencionado acima, cada signatário identificado em qualquer uma das Partes 3b-3d, conforme aplicável, afirma(m) o seguinte status de conformidade para o comerciante identificado na Parte 2 deste documento.

Selecione um:

☐	**Conforme:** Todas as seções do PCI DSS SAQ estão completas e todos os requisitos avaliados são marcados como 1) Implementados, 2) Implementados com CCW ou 3) Não Aplicável, resultando em uma classificação geral de **CONFORMIDADE**; deste modo, a *(Nome da Empresa do Comerciante)* demonstrou conformidade com todos os requisitos do PCI DSS incluídos neste SAQ, exceto aqueles indicados como Não Testado acima.
☐	**Não Conforme:** Nem todas as seções do PCI DSS SAQ estão completas ou um ou mais requisitos estão marcados como Não Implementado, resultando em uma classificação geral **NÃO CONFORME**, deste modo, a *(Nome da Empresa do Comerciante)* não demonstrou conformidade com os requisitos do PCI DSS incluídos neste SAQ. **Data Limite** para a Conformidade: *DD-MM-AAAA* Pode-se solicitar que uma entidade envie este formulário com um status Não Conforme preencha o Plano de Ação na Parte 4 deste documento. Confirme com a entidade à qual este AOC será submetido *antes de concluir a Parte 4.*
☐	**Conforme, porém com exceção Jurídica:** Um ou mais requisitos avaliados no PCI DSS SAQ são marcados como Não Implementados devido a uma restrição jurídica que impede que o requisito seja atendido e todos os outros requisitos são marcados como 1) Implementados, 2) Implementados com CCW ou 3) Não Aplicável, resultando em uma classificação geral de **CONFORME, PORÉM COM EXCEÇÃO JURÍDICA**; deste modo, a *(Nome da Empresa do Comerciante)* demonstrou conformidade com todos os requisitos do PCI DSS incluídos neste SAQ, exceto aqueles indicados como Não Implementados devido a uma restrição jurídica. Esta opção requer revisão adicional da entidade à qual este AOC será submetido. *Se selecionado, complete o seguinte:*

Requisito Afetado	Detalhes de como a restrição jurídica impede que o requisito seja atendido

Parte 3a. Reconhecimento do Comerciante

O(s) signatário(s) confirma(m):

(Selecione todos os que se aplicam)

☐	O Questionário de Autoavaliação D do PCI DSS, Versão 4.0.1 foi preenchido de acordo com as instruções nele contidas.
☐	Todas as informações contidas no SAQ mencionado acima e neste atestado representam de forma justa os resultados da avaliação do comerciante em todos os aspectos relevantes.
☐	Os controles do PCI DSS serão mantidos em todos os momentos, conforme aplicável ao ambiente do comerciante.

Parte 3b. Atestado do Comerciante

Assinatura do Diretor Executivo do Comerciante ↑	*Data: DD-MM-AAAA*
Nome do Diretor Executivo do Comerciante:	*Cargo:*

Parte 3c. Reconhecimento do Assessor de Segurança Qualificado (QSA)

Se um QSA foi envolvido ou auxiliado nesta avaliação, indique a função desempenhada:	☐ O QSA realizou procedimentos de teste.
	☐ O QSA prestou outras assistências. Se selecionado, descreva toda(s) a(s) função(ões) realizada(s):

Assinatura do QSA Líder ↑	*Data: DD-MM-AAAA*
Nome do QSA Líder:	

Assinatura do Diretor Devidamente Autorizado da Empresa do QSA ↑	*Data: DD-MM-AAAA*
Nome do Diretor Devidamente Autorizado:	*Empresa do QSA:*

Parte 3d. Envolvimento do(s) Assessor(es) de Segurança Interna (ISA) do PCI SSC

Se um(ns) ISA(s) esteve(estiveram) envolvido(s) ou auxiliado(s) nesta Avaliação, indique a função desempenhada:	☐ O(s) ISA(s) realizou(realizaram) procedimentos de teste.
	☐ O(s) ISA(s) prestou(prestaram) outras assistências. Se selecionado, descreva toda(s) a(s) função(ões) realizada(s):

Parte 4. Plano de Ação para Requisitos não Conformes

Preencha a Parte 4 somente mediante solicitação da entidade à qual este AOC será submetido e somente se a Avaliação tiver um status Não Conforme indicado na Seção 3.

Se solicitado a preencher esta seção, selecione a resposta apropriada para “Em Conformidade com os Requisitos do PCI DSS” para cada requisito abaixo. Para qualquer resposta "Não", inclua a data em que o comerciante espera estar em conformidade com o requisito e uma breve descrição das ações que estão sendo tomadas para atender ao requisito.

Requisito do PCI DSS	Descrição do Requisito	Em conformidade com os Requisitos do PCI DSS (Selecione um)		Data e Ações Corretivas (Se “NÃO” for selecionado para algum Requisito)
		SIM	NÃO	
1	Instalar e manter controles de segurança de rede	☐	☐	
2	Aplicar as configurações de segurança para todos os componentes do sistema	☐	☐	
3	Proteger os dados da conta armazenados	☐	☐	
4	Proteger os dados do titular do cartão com criptografia Forte durante a transmissão em redes públicas abertas	☐	☐	
5	Proteger todos os sistemas e redes de software malicioso	☐	☐	
6	Desenvolver e manter sistemas e software seguros	☐	☐	
7	Restringir o acesso aos componentes do sistema e aos dados do titular do cartão por necessidade de conhecimento da empresa	☐	☐	
8	Identificar usuários e autenticar o acesso aos componentes do sistema	☐	☐	
9	Restringir o acesso físico aos dados do titular do cartão	☐	☐	
10	Registrar e monitorar todo o acesso aos componentes do sistema e dados do titular do cartão	☐	☐	
11	Testar a segurança de sistemas e redes regularmente	☐	☐	
12	Apoiar a segurança da informação com políticas e programas organizacionais	☐	☐	

Apêndice A2	Requisitos Adicionais do PCI DSS para Entidades que usam SSL/TLS Antigo para Conexões de Terminal POS POI com Cartão Presente	☐	☐	

Observação: *o PCI Security Standards Council é um órgão global de padrões que fornece recursos para profissionais de segurança de pagamento desenvolvidos em colaboração com nossa comunidade de partes interessadas. Nossos materiais são aceitos em vários programas de conformidade em todo o mundo. Verifique com sua organização de aceitação de conformidade individual para garantir que este formulário seja aceitável em seu programa. Para mais informações sobre o PCI SSC e nossa comunidade de partes interessadas, visite: https://www.pcisecuritystandards.org/about_us/.*