Payment Card Industry
Padrão de Segurança de Dados

Requisitos e Procedimentos de Teste

Versão 4.0

Março de 2022

Alterações no Documento

Data	Versão	Descrição
Outubro de 2008	1.2	Apresentar o PCI DSS v1.2 como “Procedimentos de Avaliação de Requisitos de Segurança do PCI DSS”, eliminando a redundância entre documentos e fazendo alterações gerais e específicas nos Procedimentos de Auditoria de Segurança do PCI DSS v1.1. Para obter informações completas, consulte o Resumo de Alterações do Padrão de Segurança de Dados do PCI do PCI DSS versão 1.1 a 1.2.
Julho de 2009	1.2.1	Adicionar a frase que foi excluída incorretamente entre o PCI DSS v1.1 e v1.2.
		Corrigir “então” para “que” nos procedimentos de teste 6.3.7.a e 6.3.7.b.
		Remover a marcação acinzentada para as colunas "implementado" e "não implementado" no procedimento de teste 6.5.b.
		Para a Planilha de Controles de Compensação - Exemplo Completo, corrigir o texto no início da página para: “Use esta planilha para definir os controles de compensação para qualquer requisito observado como “implementado” por meio dos controles de compensação”.
Outubro de 2010	2.0	Atualizar e implementar mudanças da v1.2.1. Consulte o PCI DSS - Resumo das Alterações do PCI DSS Versão 1.2.1 a 2.0.
Novembro de 2013	3.0	Atualização da v2.0. Consulte o PCI DSS - Resumo das Alterações do PCI DSS Versão 2.0 a 3.0.
Abril de 2015	3.1	Atualização do PCI DSS v3.0. Consulte o PCI DSS - Resumo das Alterações do PCI DSS Versão 3.0 a 3.1 para obter detalhes das alterações.
Abril de 2016	3.2	Atualização do PCI DSS v3.1. Consulte o PCI DSS - Resumo das Alterações do PCI DSS Versão 3.1 a 3.2 para obter detalhes das alterações.
Maio de 2018	3.2.1	Atualização do PCI DSS v3.2. Consulte o PCI DSS – Resumo das Alterações do PCI DSS Versão 3.2 a 3.2.1 para obter detalhes das alterações.
Março de 2022	4.0	Título do documento renomeado para “Payment Card Industry Padrão de Segurança de Dados: Requisitos e Procedimentos de Teste.” Atualizado do PCI DSS v3 2.1, Consulte o PCI DSS – Resumo das Mudanças da Versão do PCI DSS 3.2.1 para 4.0 para os detalhes das mudanças.

TERMO DE RECONHECIMENTO: A versão em inglês deste documento, conforme disponibilizada no site da 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.

Índice

1 Introdução e Visão Geral do Padrão de Segurança de Dados do PCI

O Padrão de Segurança de Dados da Payment Card Industry (PCI DSS) foi desenvolvido para encorajar e aprimorar a segurança dos dados de contas de cartões de pagamento e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. O PCI DSS fornece uma linha de base de requisitos técnicos e operacionais projetados para proteger os dados da conta. Embora especificamente projetado para se concentrar em ambientes com dados de conta de cartão de pagamento, o PCI DSS também pode ser usado para proteger contra ameaças e proteger outros elementos no ecossistema de pagamento.

A Tabela 1 mostra os 12 principais requisitos do PCI DSS.

Tabela 1. Principais Requisitos do PCI DSS

Padrão de Segurança de Dados do PCI - Visão Geral de Alto Nível	
Construir e Manter uma Rede e Sistemas Seguros	**1.** Instalar e Manter Controles de Segurança de Rede. **2.** Aplicar as Configurações de Segurança para Todos os Componentes de Sistema.
Proteger os Dados da Conta	**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.
Manter um Programa de Gestão de Vulnerabilidade	**5.** Proteger Todos os Sistemas e Redes de Software Malicioso. **6.** Desenvolver e Manter Sistemas e Software Seguros.
Implementar Medidas Fortes de Controle de Acesso	**7.** Restringir o Acesso aos Componentes de Sistema e aos Dados do Titular do Cartão por Necessidade de Conhecimento do Negócio. **8.** Identificar Usuários e Autenticar o Acesso aos Componentes de Sistema **9.** Restringir o Acesso Físico aos Dados do Titular do Cartão.
Monitorar e Testar as Redes Regularmente	**10.** Registrar e Monitorar Todo o Acesso aos Componentes de Sistema e Dados do Titular do Cartão. **11.** Testar a Segurança de Sistemas e Redes Regularmente.
Manter uma Política de Segurança da Informação	**12.** Apoiar a Segurança da Informação com Políticas e Programas Organizacionais.

Este documento, Payment Card Industry Padrão de Segurança de Dados: Requisitos e Procedimentos de Teste, consiste de 12 principais requisitos do PCI DSS, requisitos de segurança detalhados, procedimentos de teste correspondentes e outras informações pertinentes a cada requisito. As seções a seguir fornecem diretrizes detalhadas e práticas recomendadas para ajudar as entidades a se preparar, conduzir e relatar os resultados de uma avaliação do PCI DSS. Os requisitos e procedimentos de teste do PCI DSS começam na página 39.

O PCI DSS compreende um conjunto mínimo de requisitos para proteger os dados da conta e pode ser aprimorado por controles e práticas adicionais para reduzir ainda mais os riscos, assim como para incorporar leis e regulamentações locais, regionais e setoriais. Além disso, a legislação ou os requisitos regulamentares podem exigir proteção específica de informações pessoais ou outros elementos de dados (por exemplo, o nome do titular do cartão).

Limitações

Se algum dos requisitos contidos neste padrão entrar em conflito com as leis do país, estado ou local, a lei do país, do estado ou do local será aplicável.

Recursos do PCI DSS

O site do PCI Security Standards Council (PCI SSC) (www.pcisecuritystandards.org) fornece os seguintes recursos adicionais para ajudar as organizações com suas avaliações e validações do PCI DSS:

- Biblioteca de Documentos, incluindo:
  - Resumo das Alterações do PCI DSS
  - Guia Rápido de Referências do PCI DSS
  - Complementos de informação e Diretrizes
  - Abordagem Priorizada para o PCI DSS
  - Modelo de Relatório do Relatório sobre Conformidade (ROC) e Instruções de Relatório
  - Questionários de Autoavaliação (SAQs) e Instruções e Diretrizes do SAQ
  - Atestados de Conformidade (*AOCs*)
- Perguntas Feitas com Frequência (FAQs)
- Site PCI para Pequenos Comerciantes
- Cursos de treinamento do PCI e webinars informativos
- Lista de Assessores de Segurança Qualificados (QSAs) e Fornecedores de Varredura Aprovados (ASVs)

- Listas de dispositivos, aplicativos e soluções aprovados do PCI

Existem mais de 60 documentos de orientação e complementos de informações disponíveis no site do PCI SSC que fornecem diretrizes e considerações específicas para o PCI DSS. Os exemplos incluem:

- Diretrizes para Escopo do PCI DSS e Segmentação de Rede
- Diretrizes de Computação em Nuvem do PCI SSC
- Diretrizes de Autenticação Multifator
- Garantia de Segurança de Terceiros
- Monitoramento Diário Efetivo
- Diretrizes de Teste de Penetração
- Melhores Práticas para Implementar um Programa de Conscientização de Segurança
- Melhores Práticas para Manter a Conformidade com o PCI DSS
- PCI DSS para Grandes Organizações
- Uso de SSL/TLS Antigo e Impacto em Varreduras ASV
- Uso de SSL/TLS Antigo para Conexões de Terminal POS POI
- Diretrizes de Segurança para Produtos de Tokenização
- Proteção de Dados de Cartão de Pagamento por Telefone

Observação: *Os Complementos de Informações complementam o PCI DSS e identificam as considerações e as recomendações adicionais para atender aos requisitos do PCI DSS. Os Complementos de Informações não substituem, suplantam ou estendem o PCI DSS ou qualquer um de seus requisitos.*

Consulte a Biblioteca de Documentos em www.pcisecuritystandards.org para obter mais informações sobre esses e outros recursos.

Além disso, consulte o Apêndice G para obter as definições dos termos do PCI DSS.

2 Informação de Aplicabilidade do PCI DSS

O PCI DSS se destina 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 do ambiente de dados do titular do cartão (CDE). Isso inclui todas as entidades envolvidas no processamento de contas de cartão de pagamento - incluindo comerciantes, processadores, adquirentes, emissores e outros prestadores de serviços.

Se alguma entidade é obrigada a cumprir ou validar sua conformidade com o PCI DSS, fica a critério das organizações que gerenciam programas de conformidade (como bandeiras de pagamento e adquirentes). Contate as organizações de interesse para todos os critérios adicionais.

Definição de Dados da Conta, Dados do Titular do Cartão e 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:

Tabela 2. Dados da Conta

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 de Serviço	• Dados de trilha completa (dados de tarja magnética ou equivalente em um chip) • Código de verificação do cartão • PINs/Blocos de PIN

Os requisitos do PCI DSS se aplicam a entidades com ambientes onde os dados da conta (dados do titular do cartão e/ou dados de autenticação confidenciais) são armazenados, processados ou transmitidos, e a entidades com ambientes que podem impactar a segurança do CDE. Alguns requisitos do PCI DSS também podem se aplicar a entidades com ambientes que não armazenam, processam ou transmitem dados da conta - por exemplo, entidades que terceirizam operações de pagamento ou gerenciamento de seu CDE[1]. As entidades que terceirizam seus ambientes de pagamento ou operações de pagamento a terceiros permanecem responsáveis por garantir que os dados da conta sejam protegidos por terceiros de acordo com os requisitos aplicáveis do PCI DSS.

[1]De acordo com as organizações que gerenciam programas de conformidade (como bandeiras de pagamento e adquirentes); as entidades devem entrar em contato com as organizações de interesse para obter mais detalhes.

O número da conta principal (PAN) é o fator determinante para os dados do titular do cartão. O termo dados da conta, portanto, abrange o seguinte: o PAN completo, quaisquer outros elementos dos dados do titular do cartão que estão presentes com o PAN e quaisquer elementos de dados de autenticação confidenciais.

Se o nome do titular do cartão, código de serviço e/ou data de validade forem armazenados, processados ou transmitidos com o PAN, ou de outra forma presentes no CDE, eles devem ser protegidos de acordo com os requisitos do PCI DSS aplicáveis aos dados do titular do cartão.

Se uma entidade armazena, processa ou transmite o PAN, então existe um CDE ao qual os requisitos do PCI DSS se aplicam. Alguns requisitos podem não ser aplicáveis, por exemplo, se a entidade não armazena o PAN, os requisitos relativos à proteção do PAN armazenado no Requisito 3 não serão aplicáveis à entidade.

Mesmo que uma entidade não armazene, processe ou transmita o PAN, alguns requisitos do PCI DSS ainda podem ser aplicáveis. Leve em consideração o seguinte:

- Se a entidade armazenar o SAD, os requisitos especificamente relacionados ao armazenamento do SAD no Requisito 3 serão aplicáveis.
- Se a entidade contratar prestadores de serviços terceirizados para armazenar, processar ou transmitir o PAN em seu nome, os requisitos relacionados ao gerenciamento de prestadores de serviços no Requisito 12 serão aplicáveis.
- Se a entidade pode impactar a segurança de um CDE porque a segurança da infraestrutura de uma entidade pode afetar como os dados do titular do cartão são processados (por exemplo, por meio de um servidor web que controla a geração de um formulário de pagamento ou página), alguns requisitos serão aplicáveis.
- Se os dados do titular do cartão estiverem presentes apenas em mídia física (por exemplo, papel), os requisitos relacionados à segurança e descarte de mídia física no Requisito 9 serão aplicáveis.
- Os requisitos relacionados a um plano de resposta a incidentes são aplicáveis a todas as entidades, para garantir que haja procedimentos a serem seguidos em caso de suspeita ou violação real da confidencialidade dos dados do titular do cartão.

Uso de Dados da Conta, Dados de Autenticação Confidenciais, Dados do Titular do Cartão e Número da Conta Principal no PCI DSS

O PCI DSS inclui requisitos que se referem especificamente aos dados da conta, dados do titular do cartão e dados de autenticação confidenciais. É importante observar que cada um desses tipos de dados é diferente e os termos não são intercambiáveis. Referências específicas nos requisitos de dados da conta, dados do titular do cartão ou dados de autenticação confidenciais são úteis e os requisitos se aplicam especificamente ao tipo de dados que é referenciado.

Elementos de Dados da Conta e Requisitos de Armazenamento

A Tabela 3 identifica os elementos dos dados do titular do cartão e dos dados de autenticação confidenciais, se o armazenamento de cada elemento de dados é permitido ou proibido e se cada elemento de dados deve ser tornado ilegível - por exemplo, com criptografia forte - quando armazenado. Esta tabela não é exaustiva e é apresentada apenas para ilustrar como os requisitos declarados se aplicam aos diferentes elementos de dados.

Tabela 3. Elementos de Dados da Conta e Requisitos de Armazenamento

		Elemento de Dados	Restrições de Armazenamento	Necessário Renderizar os Dados Armazenados Ilegíveis
Dados da Conta	**Dados do Titular do Cartão**	Número da Conta Principal (PAN)	O armazenamento é mínimo, conforme definido no Requisito 3.2	Sim, conforme definido no Requisito 3.5
		Nome do Titular do Cartão	O armazenamento é mínimo, conforme definido no Requisito 3.2[2]	Não
		Código de Serviço		
		Data de Validade		
	Dados de Autenticação Confidenciais	Dado de Trilha Completa	Não pode ser armazenado após autorização, conforme definido no Requisito 3.3.1[3]	Sim, os dados armazenados devem ser protegidos com criptografia forte até que a autorização seja concluída, conforme definido no Requisito 3.3.2
		Código de Verificação do Cartão		
		PIN/Bloco de PIN		

Se o PAN for armazenado com outros elementos dos dados do titular do cartão, apenas o PAN deve ser renderizado ilegível de acordo com o Requisito 3.5.1 do PCI DSS.

Os dados de autenticação confidenciais não devem ser armazenados após a autorização, mesmo se criptografados. Isso se aplica mesmo a ambientes onde não há PAN presente.

[2] Onde os dados existem no mesmo ambiente que o PAN.
[3] Exceto conforme permitido para emissores e empresas que oferecem suporte a serviços de emissão. Os requisitos para emissores e serviços de emissão são definidos separadamente no Requisito 3.3.3.

3 Relação entre o PCI DSS e os Padrões de Software do PCI SSC

O PCI SSC oferece suporte ao uso de software de pagamento seguro em ambientes de dados do titular do cartão (CDE) por meio do Padrão de Segurança de Dados do Aplicativo de Pagamento (PA-DSS) e da Estrutura de Segurança de Software (SSF), que consiste no Padrão de Software Seguro e no Padrão de Ciclo de Vida do Software Seguro (SLC Seguro). O software que é validado e listado pelo PCI SSC fornece garantia de que o software foi desenvolvido usando práticas seguras e atendeu a um conjunto definido de requisitos de segurança de software.

Os programas de software seguro do PCI SSC incluem listas de software de pagamento e fornecedores de software que foram validados como cumprindo os padrões de software do PCI SSC aplicáveis.

- **Software Validado**: O software de pagamento listado no site do PCI SSC como um aplicativo de pagamento validado (PA-DSS) ou um software de pagamento validado (o padrão de software seguro) foi analisado por um assessor qualificado a fim de confirmar se o software atende aos requisitos de segurança desse padrão. Os requisitos de segurança desses padrões se concentram na proteção da integridade e confidencialidade das transações de pagamento e dos dados da conta.
- **Fornecedores de Software Validado**: O Padrão de SLC Seguro define requisitos de segurança para fornecedores de software para integrar práticas seguras de desenvolvimento de software em todo o seu ciclo de vida. Os fornecedores de software que foram validados como atendendo ao Padrão de SLC Seguro estão listados no site do PCI SSC como Fornecedor Qualificado de SLC Seguro.

Observação: *O PA-DSS e o programa relacionado serão desativados em outubro de 2022. Consulte a lista de aplicativos de pagamento validados do PCI SSC para obter as datas de validade dos aplicativos validados do PA-DSS. Após a data de expiração, os aplicativos são listados como "Aceitável apenas para Implantações Pré-Existentes". Se uma entidade pode continuar a usar um aplicativo PA-DSS expirado, fica a critério das organizações que gerenciam programas de conformidade (como bandeiras de pagamento e adquirentes); as entidades devem entrar em contato com as organizações de interesse para obter mais detalhes.*

Para obter mais informações sobre o SSF ou PA-DSS, consulte os respectivos Guias de Programa em www.pcisecuritystandards.org.

Todo software que armazena, processa ou transmite dados da conta, ou que poderia impactar a segurança dos dados da conta ou um CDE, está no escopo da avaliação do PCI DSS de uma entidade. Embora o uso de software de pagamento validado ofereça suporte à segurança do CDE de uma entidade, o uso de tal software por si só não torna uma entidade em conformidade com o PCI DSS. A avaliação do PCI DSS da entidade deve incluir a verificação de que o software está configurado corretamente e implementado com segurança para oferecer suporte aos requisitos aplicáveis do PCI DSS. Além disso, se o software de pagamento listado no PCI tiver sido personalizado, uma análise mais aprofundada será necessária durante a avaliação do PCI DSS, pois o software pode não ser mais representativo da versão que foi originalmente validada.

Como as ameaças à segurança estão em constante evolução, o software que não tem mais suporte do fornecedor (por exemplo, identificado pelo fornecedor como "fim de vida") pode não oferecer o mesmo nível de segurança que as versões com suporte. As entidades são fortemente encorajadas a manter seus softwares na versão mais atual e atualizados com as versões de software mais recentes disponíveis.

As entidades que desenvolvem seu próprio software são encorajadas a consultar os padrões de segurança de software do PCI SSC e considerar os requisitos neles contidos como as práticas recomendadas para uso em seus ambientes de desenvolvimento. O software de pagamento seguro implementado em um ambiente em conformidade com o PCI DSS ajudará a minimizar o potencial de violações de segurança que levam ao comprometimento dos dados da conta e fraudes. Consulte Software Sob Medida e Personalizado.

Aplicabilidade do PCI DSS para Fornecedores de Software de Pagamento

O PCI DSS pode se aplicar a um fornecedor de software de pagamento se o fornecedor também for um prestador de serviços que armazena, processa ou transmite dados da conta, ou tem acesso aos dados da conta de seus clientes - por exemplo, na função de um prestador de serviços de pagamento ou via acesso remoto ao ambiente do cliente. Os fornecedores de software aos quais o PCI DSS pode ser aplicável incluem aqueles que oferecem serviços de pagamento, bem como prestadores de serviços em nuvem que oferecem terminais de pagamento na nuvem, software como serviço (SaaS), comércio eletrônico na nuvem e outros serviços de pagamento na nuvem.

Software Sob Medida e Personalizado

Todo software sob medida e personalizado que armazena, processa ou transmite dados da conta, ou que poderia impactar na segurança dos dados da conta ou um CDE, está no escopo da avaliação do PCI DSS de uma entidade.

O software sob medida e personalizado que foi desenvolvido e mantido de acordo com um dos padrões da Estrutura de Segurança de Software do PCI SSC (o Padrão de Software Seguro ou o Padrão de SLC Seguro) apoiará uma entidade no cumprimento do Requisito 6 do PCI DSS.

Consulte o Apêndice F para obter mais detalhes.

Observação: *O Requisito 6 do PCI DSS se aplica totalmente ao software sob medida e personalizado que não foi desenvolvido e mantido de acordo com um dos padrões da Estrutura de Segurança de Software do PCI SSC. As entidades que usam fornecedores de software para desenvolver software sob medida ou personalizado que podem afetar a segurança dos dados da conta ou seu CDE são responsáveis por garantir que esses fornecedores de software desenvolvam o software de acordo com o Requisito 6 do PCI DSS.*

4 Escopo dos Requisitos do PCI DSS

Os requisitos do PCI DSS se aplicam a:

- O ambiente de dados do titular do cartão (CDE), que é composto por:
  - Componentes de sistema, pessoas e processos que armazenam, processam e transmitem dados do titular do cartão e/ou dados de autenticação confidenciais e
  - Componentes de sistema que podem não armazenar, processar ou transmitir o CHD/SAD, mas têm conectividade irrestrita aos componentes de sistema que armazenam, processam ou transmitem o CHD/SAD.

E

- Componentes de sistema, pessoas e processos que podem impactar a segurança do CDE.[4]

"Componentes de sistema" incluem dispositivos de rede, servidores, dispositivos de computação, componentes virtuais, componentes de nuvem e software. Exemplos de componentes de sistema incluem, mas não estão limitados a:

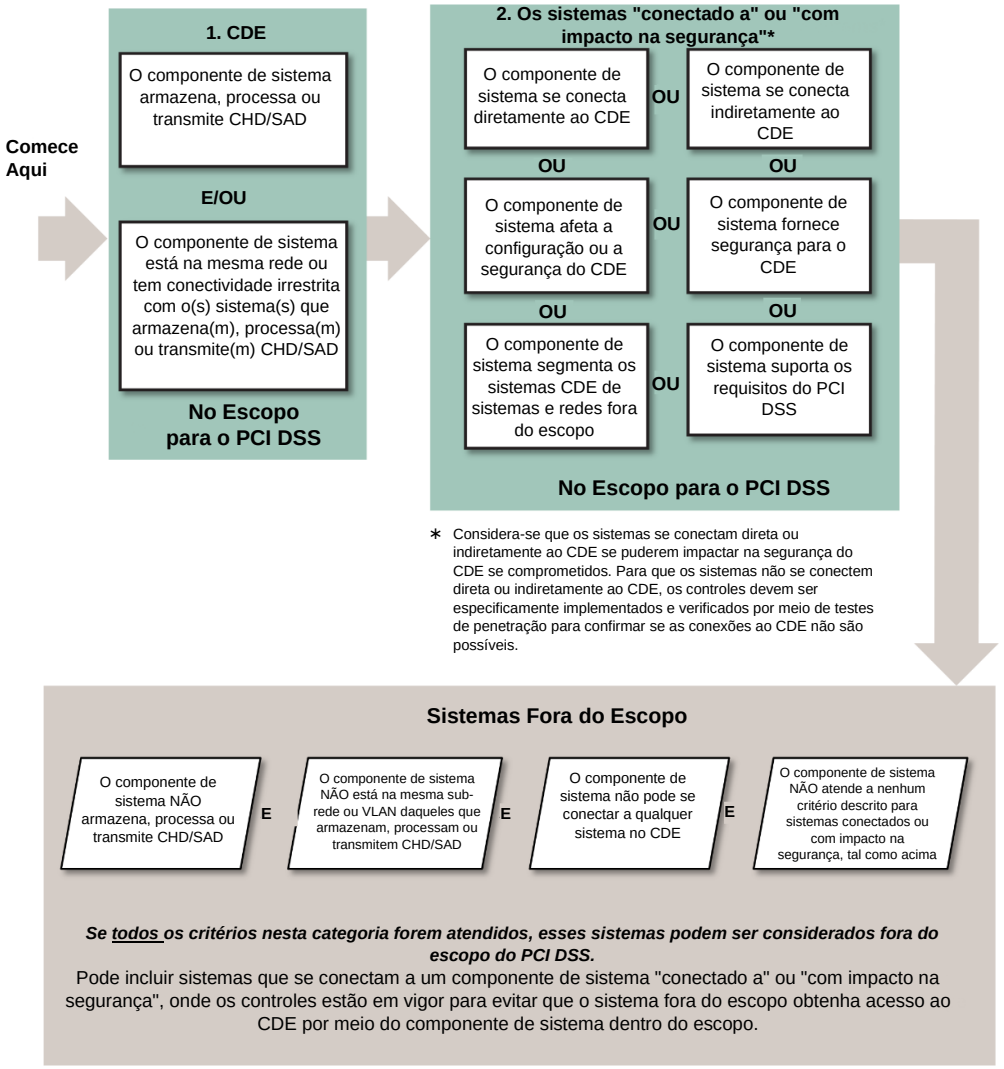
- Sistemas que armazenam, processam ou transmitem dados da conta (por exemplo, terminais de pagamento, sistemas de autorização, sistemas de compensação, sistemas de middleware de pagamento, sistemas de back-office de pagamento, carrinho de compras e sistemas de frente de loja, portal de pagamento/sistemas de comutação, sistemas de monitoramento de fraude).
- Sistemas que fornecem serviços de segurança (por exemplo, servidores de autenticação, servidores de controle de acesso, sistemas de gerenciamento de informações e eventos de segurança (SIEM), sistemas de segurança física (por exemplo, acesso por crachá ou CFTV), sistemas de autenticação multifator, sistemas antimalware).
- Sistemas que facilitam a segmentação (por exemplo, controles de segurança de rede interna).
- Sistemas que podem afetar a segurança dos dados da conta ou do CDE (por exemplo, resolução de nome ou servidores de redirecionamento de comércio eletrônico (web)).
- Componentes de virtualização, como máquinas virtuais, switches/roteadores virtuais, dispositivos virtuais, aplicativos/desktops virtuais e hypervisors.
- Infraestrutura e componentes de nuvem, tanto externos quanto locais, incluindo instanciações de contêineres ou imagens, nuvens privadas virtuais, identidade baseada em nuvem e gerenciamento de acesso, CDEs residentes no local ou na nuvem, malhas de serviço com aplicativos em contêineres e ferramentas de orquestração de contêineres.

[4] Para obter orientações adicionais, consulte o *Complemento de Informações: Diretrizes para Escopo do PCI DSS e Segmentação de Rede* no site do PCI SSC.

- Componentes de rede, incluindo, mas não se limitando a, controles de segurança de rede, switches, roteadores, dispositivos de rede VoIP, pontos de acesso sem fio, dispositivos de rede e outros dispositivos de segurança.
- Tipos de servidor, incluindo, mas não se limitando a web, aplicativo, banco de dados, autenticação, e-mail, proxy, Protocolo de Tempo de Rede (NTP) e Sistema de Nome de Domínio (DNS).
- Dispositivos de usuário final, como computadores, laptops, estações de trabalho, estações de trabalho administrativas, tablets e dispositivos móveis.
- Impressoras e dispositivos multifuncionais que digitalizam, imprimem e enviam fax.
- Armazenamento de dados da conta em qualquer formato (por exemplo, papel, arquivos de dados, arquivos de áudio, imagens e gravações de vídeo).
- Aplicativos, software e componentes de software, aplicativos sem servidor, incluindo todos os adquiridos, assinados (por exemplo, “Software-as-a-Service [Software-como-um-Serviço]”), software sob medida e personalizado, incluindo aplicativos internos e externos (por exemplo, disponível para Internet).
- Ferramentas, repositórios de código e sistemas que implementam gerenciamento de configuração de software ou para implantação de objetos no CDE ou em sistemas que podem impactar o CDE.

A Figura 1 mostra as considerações para determinar o escopo dos componentes de sistema para o PCI DSS.

Figura 1. Compreendendo o Escopo do PCI DSS



Confirmação Anual de Escopo do PCI DSS

A primeira etapa na preparação para uma avaliação do PCI DSS é a entidade determinar com precisão o escopo da revisão. A entidade avaliada deve confirmar a precisão de seu escopo do PCI DSS de acordo com o Requisito 12.5.2 do PCI DSS, identificando todos os locais e fluxos de dados da conta e identificando todos os sistemas que estão conectados ou, se comprometidos, podem impactar o CDE (por exemplo, servidores de autenticação, servidores de acesso remoto, servidores de registro) para garantir que estejam incluídos no escopo do PCI DSS. Todos os tipos de sistemas e locais devem ser considerados durante o processo de definição do escopo, incluindo sites de backup/recuperação e sistemas de falha.

As etapas mínimas para uma entidade confirmar a precisão de seu escopo do PCI DSS são especificadas no Requisito 12.5.2 do PCI DSS. A entidade deve reter a documentação para mostrar como foi determinado o escopo do PCI DSS. A documentação é retida para análise do assessor e para referência durante a próxima atividade de confirmação de escopo do PCI DSS da entidade. Para cada avaliação do PCI DSS, o assessor valida se a entidade definiu e documentou com precisão o escopo da avaliação.

***Observação**: Esta confirmação anual do escopo do PCI DSS é definida no Requisito do PCI DSS em 12.5.2 e é uma atividade que deve ser realizada pela entidade. Esta atividade não é a mesma, nem se destina a ser substituída pela confirmação de escopo realizada pelo assessor da entidade durante a avaliação.*

Segmentação

A segmentação (ou isolamento) do CDE do restante da rede de uma entidade não é um requisito do PCI DSS. Entretanto, é altamente recomendado como um método que pode reduzir o:

- Escopo da avaliação do PCI DSS
- Custo da avaliação do PCI DSS
- Custo e dificuldade de implementação e manutenção de controles do PCI DSS
- Risco para uma organização em relação aos dados da conta do cartão de pagamento (reduzido pela consolidação desses dados em menos locais mais controlados)

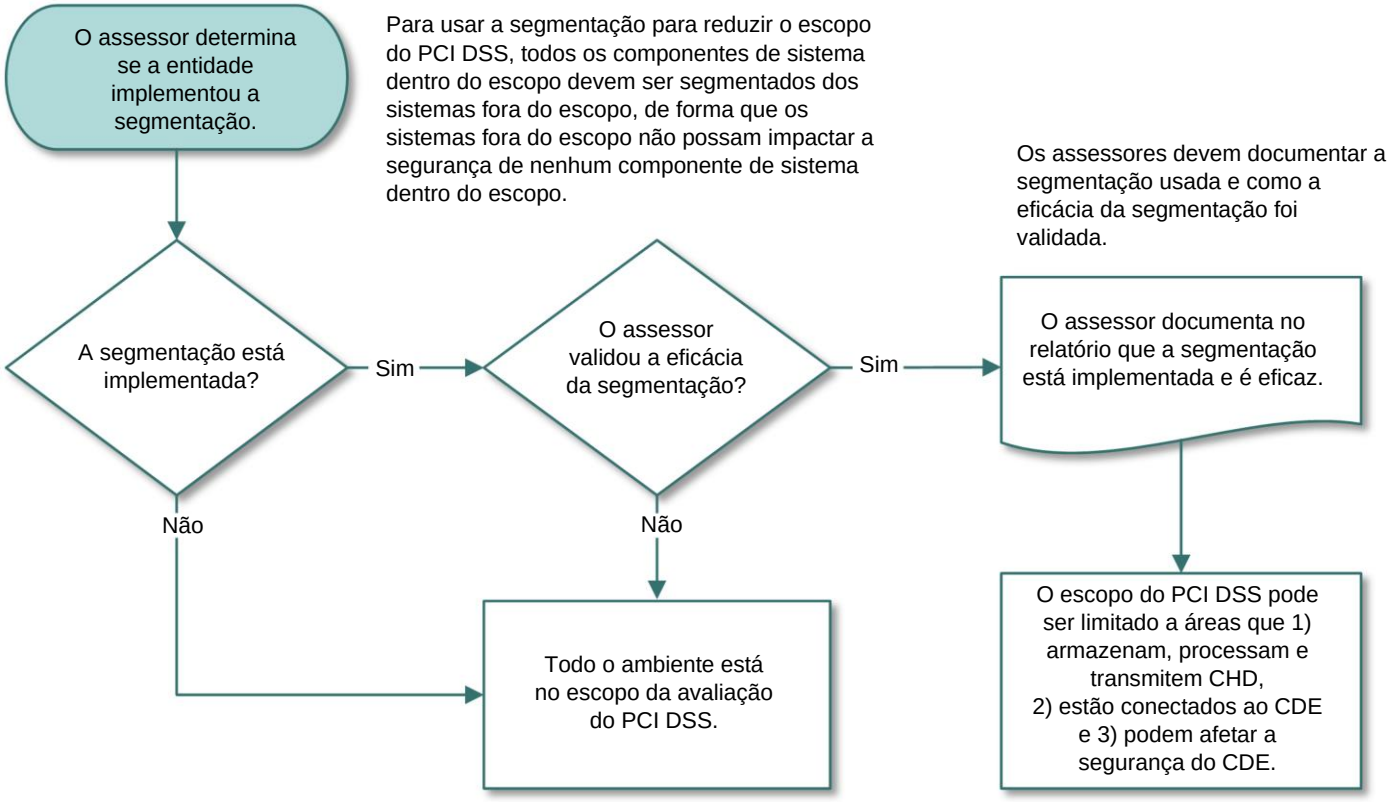
Sem segmentação adequada (às vezes chamada de "rede plana"), toda a rede está no escopo da avaliação do PCI DSS. A segmentação pode ser alcançada usando vários métodos físicos ou lógicos, como controles de segurança de rede interna configurados corretamente, roteadores com listas de controle de acesso fortes ou outras tecnologias que restringem o acesso a um segmento específico de uma rede. Para ser considerado fora do escopo do PCI DSS, um componente de sistema deve ser devidamente segmentado (isolado) do CDE, de forma que o componente de sistema fora do escopo não possa impactar a segurança do CDE, mesmo se esse componente estiver comprometido.

Um pré-requisito importante para reduzir o escopo do CDE é um entendimento claro das necessidades e processos de negócios relacionados ao armazenamento, processamento e transmissão de dados da conta. Restringir os dados da conta ao mínimo de locais possível, eliminando dados desnecessários e consolidando os dados necessários, pode exigir a reengenharia de práticas comerciais de longa data.

A documentação dos fluxos de dados da conta por meio de um diagrama de fluxo de dados ajuda uma entidade a compreender totalmente como os dados da conta chegam à organização, onde residem na organização e como passam por vários sistemas dentro da organização. Os diagramas de fluxo de dados também ilustram todos os locais onde os dados da conta são armazenados, processados e transmitidos. Essas informações apoiam na implementação da segmentação de uma entidade e também podem apoiar na confirmação de que a segmentação está sendo usada para isolar o CDE de redes fora do escopo.

Se a segmentação for usada para reduzir o escopo da avaliação do PCI DSS, o assessor deve verificar se a segmentação é adequada para reduzir o escopo da avaliação, conforme ilustrado na Figura 2. Em um alto nível, a segmentação adequada isola os sistemas que armazenam, processam ou transmitem dados da conta daqueles que não o fazem. Entretanto, a adequação de uma implementação de segmentação específica é altamente variável e depende de vários fatores, como a configuração de uma determinada rede, as tecnologias implementadas e outros controles que podem ser implementados.

Figura 2. Segmentação e Impacto no Escopo do PCI DSS



Wireless

Se a tecnologia wireless for usada para armazenar, processar ou transmitir dados da conta (por exemplo, dispositivos de ponto de venda wireless) ou se uma rede local wireless (WLAN) fizer parte ou estiver conectada ao CDE, os requisitos do PCI DSS e procedimentos de teste para proteger ambientes wireless se aplicam e devem ser executados.

A detecção de tecnologia wireless não autorizada deve ser realizada de acordo com o Requisito 11.2.1 do PCI DSS, mesmo quando a rede wireless não é usada no CDE e a entidade tem uma política que proíbe o uso de tecnologia wireless em seu ambiente. Isso se deve à facilidade com que um ponto de acesso wireless pode ser conectado a uma rede, à dificuldade em detectar sua presença e ao aumento do risco apresentado por dispositivos wireless não autorizados.

Antes de a tecnologia wireless ser implementada, uma entidade deve avaliar cuidadosamente a necessidade da tecnologia em relação ao risco. Considere a implantação de tecnologia wireless apenas para transmissão de dados não confidenciais.

Dados do Titular do Cartão Criptografados e Impacto no Escopo do PCI DSS

A criptografia dos dados do titular do cartão com criptografia forte é um método aceitável para tornar os dados ilegíveis de acordo com o Requisito 3.5 do PCI DSS. No entanto, a criptografia sozinha geralmente é insuficiente para tornar os dados do titular do cartão fora do escopo do PCI DSS e não remove a necessidade do PCI DSS nesse ambiente. O ambiente da entidade ainda está dentro do escopo do PCI DSS devido à presença de dados do titular do cartão. Por exemplo, para um comerciante com ambiente com cartão presente, há acesso físico aos cartões de pagamento para concluir uma transação e também pode haver relatórios ou recibos em papel com os dados do titular do cartão. Da mesma forma, em comerciantes com ambientes sem presença de cartão, como “mail-order/telephone-order [pedido por telefone/correio]” e comércio eletrônico, os detalhes do cartão de pagamento são fornecidos por meio de canais que precisam ser avaliados e protegidos de acordo com o PCI DSS.

Os itens a seguir estão no escopo do PCI DSS:

- Sistemas que executam criptografia e/ou descriptografia dos dados do titular do cartão e sistemas que executam funções de gerenciamento de chaves,
- Dados do titular do cartão criptografados que não estão isolados dos processos de criptografia e descriptografia e gerenciamento de chaves,
- Dados do titular do cartão criptografados que estão presentes em um sistema ou mídia que também contém a chave de descriptografia,
- Dados do titular do cartão criptografados que estão presentes no mesmo ambiente que a chave de descriptografia,
- Dados do titular do cartão criptografados que podem ser acessados por uma entidade que também tem acesso à chave de descriptografia.

***Observação**: Uma solução P2PE listada no PCI pode reduzir significativamente o número de requisitos do PCI DSS aplicáveis ao ambiente de dados do titular do cartão de um comerciante. Não obstante, isso não remove completamente a aplicabilidade do PCI DSS no ambiente do comerciante.*

Dados do Titular do Cartão Criptografados e Impacto no Escopo do PCI DSS para Prestadores de Serviços Terceirizados

Quando um prestador de serviços terceirizado (TPSP) recebe e/ou armazena apenas dados criptografados por outra entidade, e onde eles não têm a capacidade de descriptografar os dados, o TPSP pode ser capaz de considerar os dados criptografados fora do escopo caso certas condições sejam atendidas. Isso ocorre porque a responsabilidade pelos dados geralmente permanece com a entidade, ou entidades, com a capacidade de descriptografar os dados ou impactar a segurança dos dados criptografados. Determinar qual parte é responsável pelos controles do PCI DSS específicos dependerá de vários fatores, incluindo quem tem acesso às chaves de descriptografia, a função desempenhada por cada parte e o acordo entre as partes. As responsabilidades devem ser claramente definidas e documentadas para garantir que tanto o TPSP quanto a entidade que fornece os dados criptografados entendam qual entidade é responsável por quais controles de segurança.

Por exemplo, um TPSP que presta serviços de armazenamento recebe e armazena dados criptografados do titular do cartão fornecidos pelos clientes para fins de backup. Este TPSP não tem acesso às chaves de criptografia ou descriptografia, nem executa nenhum gerenciamento de chaves para seus clientes. O TPSP pode excluir quaisquer dados criptografados ao determinar seu escopo do PCI DSS. Entretanto, o TPSP mantém a responsabilidade de controlar o acesso ao armazenamento de dados criptografados como parte de seus contratos de serviço com seus clientes.

A responsabilidade por garantir que os dados criptografados e as chaves criptográficas sejam protegidos de acordo com os requisitos aplicáveis do PCI DSS geralmente é compartilhada entre as entidades. No exemplo acima, o cliente determina quem de seu pessoal está autorizado a acessar a mídia de armazenamento, e a instalação de armazenamento é responsável por gerenciar os controles de acesso físico e/ou lógico para garantir que apenas pessoas autorizadas pelo cliente tenham acesso à mídia de armazenamento. Os requisitos específicos do PCI DSS aplicáveis a um TPSP dependerão dos serviços prestados e do acordo entre as duas partes. No exemplo de um TPSP que presta serviços de armazenamento, os controles de acesso físico e lógico fornecidos pelo TPSP precisarão ser revisados pelo menos uma vez por ano. Esta revisão pode ser realizada como parte da avaliação do PCI DSS do comerciante ou, alternativamente, a revisão pode ser realizada e os controles validados pelo TPSP com as evidências adequadas fornecidas ao comerciante. Para obter informações sobre "evidências apropriadas", consulte Opções para TPSPs Validarem a Conformidade com o PCI DSS para Serviços do TPSP que Atendem aos Requisitos do PCI DSS dos Clientes.

Como outro exemplo, um TPSP que recebe apenas dados do titular do cartão criptografados para fins de roteamento para outras entidades, e que não tem acesso aos dados ou chaves criptográficas, pode não ter qualquer responsabilidade no PCI DSS por esses dados criptografados. Nesse cenário, onde o TPSP não está prestando nenhum serviço de segurança ou controle de acesso, eles podem ser

considerados o mesmo que uma rede pública ou não confiável, e seria de responsabilidade da(s) entidade(s) enviar/receber dados da conta por meio das redes de TPSP para garantir que os controles do PCI DSS sejam aplicados para proteger os dados que estão sendo transmitidos.

Uso de Prestadores de Serviço Terceirizados

Uma entidade (referida como o "cliente" nesta seção) pode escolher usar um prestador de serviços terceirizado (TPSP) para armazenar, processar ou transmitir dados da conta ou para gerenciar componentes de sistema no escopo em nome do cliente. O uso de um TPSP pode ter um impacto na segurança do CDE de um cliente.

***Observação**: O uso de um TPSP em conformidade com PCI DSS não torna um cliente em conformidade com o PCI DSS, nem remove a responsabilidade do cliente por sua própria conformidade com o PCI DSS. Mesmo se um cliente usar um TPSP para atender a todas as funções de dados da conta, esse cliente continua responsável por confirmar sua própria conformidade, tal como solicitado por organizações que gerenciam programas de conformidade (por exemplo, bandeiras de pagamento e adquirentes). Os clientes devem entrar em contato com as organizações de interesse para quaisquer requisitos.*

Usando os TPSPs e o Impacto nos Clientes para Atendimento ao Requisito 12.8 do PCI DSS

Existem muitos cenários diferentes onde um cliente pode usar um ou mais TPSPs para funções dentro ou relacionadas ao CDE do cliente. Em todos os cenários onde um TPSP é usado, o cliente deve gerenciar e supervisionar o status de conformidade do PCI DSS de todos os seus TPSPs de acordo com o Requisito 12.8, incluindo os TPSPs que:

- Têm acesso ao CDE do cliente,
- Gerenciam componentes do sistema dentro do escopo em nome do cliente e/ou
- Podem impactar a segurança do CDE do cliente.

Gerenciar os TPSPs de acordo com o Requisito 12.8 inclui a realização de *due diligence*, ter acordos apropriados em vigor, identificar quais requisitos se aplicam ao cliente e quais se aplicam ao TPSP e monitorar o status de conformidade dos TPSPs pelo menos uma vez por ano.

O Requisito 12.8 não especifica que os TPSPs do cliente devem estar em conformidade com o PCI DSS, apenas que o cliente monitora seu status de conformidade de acordo com o especificado no requisito. Portanto, um TPSP não precisa estar em conformidade com o PCI DSS para que seu cliente atenda ao Requisito 12.8.

Impacto do uso dos TPSPs para serviços que atendem aos requisitos do PCI DSS dos clientes

Quando o TPSP fornece um serviço que atende a um ou mais requisitos do PCI DSS em nome do cliente ou onde esse serviço pode afetar a segurança do CDE do cliente, esses requisitos estão no escopo da avaliação do cliente e a conformidade desse serviço terá

impacto na conformidade do PCI DSS do cliente. O TPSP deve demonstrar que atende aos requisitos do PCI DSS aplicáveis para que esses requisitos estejam implementados para seus clientes. Por exemplo, se uma entidade contrata um TPSP para gerenciar seus controles de segurança de rede, e o TPSP não fornece evidências de que atende aos requisitos aplicáveis no Requisito 1 do PCI DSS, então esses requisitos não estão implementados para a avaliação do cliente. Como outro exemplo, os TPSPs que armazenam backups dos dados do titular do cartão em nome dos clientes precisariam atender aos requisitos aplicáveis relacionados a controles de acesso, segurança física, etc., para que seus clientes considerassem esses requisitos implementados para suas avaliações.

Importância da compreensão das responsabilidades entre clientes e TPSPs

Os clientes e TPSPs devem identificar e compreender claramente o seguinte:

- Os serviços e componentes de sistema incluídos no escopo da avaliação PCI DSS do TPSP,
- Os requisitos e sub-requisitos específicos do PCI DSS cobertos pela avaliação do PCI DSS do TPSP,
- Quaisquer requisitos que são de responsabilidade dos clientes para incluir em suas próprias avaliações do PCI DSS, e
- Quaisquer requisitos do PCI DSS cuja responsabilidade seja compartilhada entre o TPSP e seus clientes.

Por exemplo, um provedor de nuvem deve definir claramente quais de seus endereços IP são verificados como parte de seu processo de verificação de vulnerabilidade trimestral e quais endereços IP são de responsabilidade de seus clientes para verificarem as vulnerabilidades.

De acordo com o Requisito 12.9.2, os TPSPs são obrigados a apoiar as solicitações de seus clientes para obter informações sobre o status de conformidade do PCI DSS do TPSP relacionado aos serviços prestados aos clientes e sobre quais requisitos do PCI DSS são de responsabilidade do TPSP, quais são de responsabilidade do cliente e quaisquer responsabilidades entre o cliente e o TPSP. Consulte *Dicas e Ferramentas para Compreender o PCI DSS v4*.0 para obter um modelo de matriz de responsabilidade que pode ser usado para documentar e esclarecer como as responsabilidades são compartilhadas entre os TPSPs e os clientes.

Opções para TPSPs validarem a conformidade com o PCI DSS para serviços do TPSP que atendem aos requisitos do PCI DSS dos clientes

Os TPSPs são responsáveis por demonstrar sua conformidade com o PCI DSS conforme solicitado por organizações que gerenciam programas de conformidade (por exemplo, bandeiras de pagamento e adquirentes). Os TPSPs devem entrar em contato com as organizações de interesse para quaisquer requisitos.

Quando um TPSP fornece serviços que se destinam a atender ou facilitar o atendimento aos requisitos do PCI DSS de um cliente ou que podem impactar a segurança do CDE de um cliente, esses requisitos estão no escopo das avaliações do PCI DSS do cliente. Existem duas opções para os TPSPs validarem a conformidade neste cenário:

- **Avaliação anual**: o TPSP passa por uma(s) avaliação(ões) anual(is) do PCI DSS e fornece evidências aos seus clientes para demonstrar que o TPSP atende aos requisitos aplicáveis do PCI DSS; ou

- **Avaliações múltiplas sob demanda**: Se um TPSP não passar por uma avaliação anual do PCI DSS, ele deve passar por avaliações mediante solicitação de seus clientes e/ou participar de cada uma das avaliações do PCI DSS de seus clientes, com os resultados de cada revisão fornecida para o(s) respectivo(s) cliente(s).

Se o TPSP passar por sua própria avaliação do PCI DSS, espera-se que forneça evidências suficientes aos seus clientes para verificar se o escopo da avaliação do PCI DSS do TPSP cobriu os serviços aplicáveis ao cliente, e se foi examinado e determinado que os requisitos relevantes do PCI DSS estão implementados. Se o prestador tiver um Atestado de Conformidade do PCI DSS (AOC), espera-se que o TPSP forneça o AOC aos clientes mediante solicitação. O cliente também pode solicitar seções relevantes do Relatório de Conformidade (ROC) do PCI DSS do TPSP. O ROC pode ser redigido para proteger qualquer informação confidencial.

Se o TPSP não passar por sua própria avaliação do PCI DSS e, portanto, não tiver um AOC, espera-se que o TPSP forneça evidências específicas relacionadas aos requisitos aplicáveis do PCI DSS, para que o cliente (ou seu assessor) seja capaz de confirmar se o TPSP está atendendo a esses requisitos do PCI DSS.

Presença de TPSPs em uma(s) lista(s) de Prestadores de Serviços em Conformidade com o PCI DSS da(s) bandeira(s) de pagamento

Para um cliente que está monitorando o status de conformidade de um TPSP de acordo com o Requisito 12.8, a presença do TPSP em uma lista de prestadores de serviços em conformidade com PCI DSS da bandeira de pagamento ***pode ser evidência suficiente*** do status de conformidade do TPSP se estiver claro na lista que os serviços aplicáveis para o cliente foram cobertos pela avaliação do PCI DSS do TPSP. Se não estiver claro na lista, o cliente deve obter outra confirmação por escrito que aborde o status de conformidade do PCI DSS do TPSP.

Para um cliente que está procurando evidências de conformidade com o PCI DSS para requisitos que um TPSP atende em nome do cliente ou onde o serviço prestado pode afetar a segurança do CDE do cliente, a presença do TPSP em uma lista de prestadores de serviços em conformidade com o PCI DSS das bandeiras de pagamento ***não é evidência suficiente*** de que os requisitos aplicáveis do PCI DSS para esse TPSP foram incluídos na avaliação. Se o TPSP tiver um AOC do PCI DSS, espera-se que ele seja fornecido aos clientes mediante solicitação.

5 Melhores Práticas para a Implementação do PCI DSS em Processos de Negócios Habituais

Uma entidade que implementa processos de negócios habituais, também conhecidos como BAU, como parte de sua estratégia de segurança geral está tomando medidas para garantir que os controles de segurança que foram implementados para proteger os dados e um ambiente continuem a ser implementados corretamente e funcionando adequadamente no curso normal dos negócios.

Alguns requisitos do PCI DSS têm como objetivo atuar como processos BAU, monitorando os controles de segurança para garantir sua eficácia em uma base contínua. Essa supervisão da entidade auxilia no fornecimento de garantia razoável de que a conformidade de seu ambiente é preservada entre as avaliações do PCI DSS. Embora existam atualmente alguns requisitos de BAU definidos no padrão, uma entidade deve adotar processos BAU adicionais específicos para sua organização e ambiente, quando possível. Os processos BAU são uma forma de verificar se os controles automatizados e manuais estão funcionando conforme o esperado. Independentemente de o requisito do PCI DSS ser automatizado ou manual, é importante que os processos BAU detectem anomalias e alertem e relatem para que os indivíduos responsáveis tratem da situação em tempo hábil.

Exemplos de como o PCI DSS deve ser incorporado às atividades BAU incluem, mas não estão limitadas a:

- Atribuindo responsabilidade geral e prestação de contas pela conformidade com o PCI DSS a um indivíduo ou a uma equipe. Pode incluir um estatuto definido pela gerência executiva para um programa de conformidade do PCI DSS específico e comunicação à gerência executiva.
- Desenvolvendo métricas de desempenho para medir a eficácia das iniciativas de segurança e monitoramento contínuo dos controles de segurança, incluindo aqueles que são altamente considerados, como controles de segurança de rede, sistemas de detecção de intrusão/sistemas de prevenção de intrusão (IDS/IPS), mecanismos de detecção de mudança, soluções antimalware e controles de acesso, para garantir que estejam operando de forma eficaz e conforme o pretendido.
- Revisando os dados registrados com mais frequência para obter insights sobre tendências ou comportamentos que podem não ser óbvios apenas com o monitoramento.
- Garantindo que todas as falhas nos controles de segurança sejam detectadas e respondidas prontamente. Os processos para responder a falhas de controle de segurança devem incluir:
  - Restauração do controle de segurança.
  - Identificação da causa da falha.
  - Identificação e resolução de quaisquer problemas de segurança que surgiram durante a falha do controle de segurança.
  - Implementação de mitigação, como processos ou controles técnicos, para evitar que a causa da falha se repita.
  - Retomada do monitoramento do controle de segurança, talvez com monitoramento aprimorado por um período de tempo, para verificar se o controle está operando de forma eficaz.

- Revisão das mudanças que podem introduzir riscos de segurança ao ambiente (por exemplo, adição de novos sistemas, mudanças em sistemas ou configurações de rede) antes de concluir a mudança, incluindo o seguinte:
  - Execução de uma avaliação de risco para determinar o impacto potencial no escopo do PCI DSS (por exemplo, uma nova regra do controle de segurança de rede que permite a conectividade entre um sistema no CDE e outro sistema pode trazer sistemas ou redes adicionais para o escopo do PCI DSS).
  - Identificação dos requisitos do PCI DSS aplicáveis aos sistemas e redes afetados pelas mudanças (por exemplo, se um novo sistema estiver no escopo do PCI DSS, ele precisará ser configurado de acordo com os padrões de configuração do sistema, incluindo mecanismos de detecção de mudança, software antimalware, patches e registro de auditoria. Esses novos sistemas e redes precisariam ser adicionados ao inventário de componentes do sistema dentro do escopo e ao cronograma de varredura de vulnerabilidades trimestral).
  - Atualização do escopo do PCI DSS e implementação de controles de segurança conforme apropriado.
  - Atualização da documentação para refletir as mudanças implementadas.
- Revisão do impacto no escopo e requisitos do PCI DSS com as mudanças na estrutura organizacional (por exemplo, fusão ou aquisição de uma empresa).
- Revisão de conexões externas e acesso de terceiros periodicamente.
- Para entidades que usam terceiros para desenvolvimento de software, confirmar periodicamente se essas atividades de desenvolvimento de software continuam a cumprir com os requisitos de desenvolvimento de software no Requisito 6.
- Realização das análises periódicas para confirmar se os requisitos do PCI DSS continuam implementados e se o pessoal segue os processos estabelecidos. As revisões periódicas devem abranger todas as instalações e locais, incluindo pontos de venda e centros de dados, sejam autogerenciados ou se um TPSP for usado. Por exemplo, revisões periódicas podem ser usadas para confirmar que os padrões de configuração foram aplicados aos sistemas aplicáveis, as contas e as senhas de fornecedores padrão foram removidas ou desabilitadas, patches e soluções antimalware estão atualizados, registros de auditoria estão sendo revisados e assim por diante. A frequência das revisões periódicas deve ser determinada pela entidade conforme apropriado para o tamanho e a complexidade de seu ambiente, salvo indicação em contrário no PCI DSS.

Essas revisões também podem ser usadas para verificar se as evidências necessárias para uma avaliação do PCI DSS estão sendo mantidas. Por exemplo, evidências de registros de auditoria, relatórios de varredura de vulnerabilidade e revisões de conjuntos de regras de controle de segurança de rede são necessários para ajudar a entidade a se preparar para sua próxima avaliação do PCI DSS.

- Estabelecer comunicação com todas as partes afetadas, externas e internas, sobre ameaças recém-identificadas e mudanças na estrutura da organização. Os materiais de comunicação devem ajudar os destinatários a compreender o impacto das ameaças, etapas de atenuação e pontos de contato para obter mais informações ou escalação.
- Revisão das tecnologias de hardware e software pelo menos uma vez a cada 12 meses para confirmar se continuam a ter suporte do fornecedor e podem atender aos requisitos de segurança da entidade, incluindo o PCI DSS. Se as tecnologias não

forem mais suportadas pelo fornecedor ou não puderem atender às necessidades de segurança da entidade, a entidade deve preparar um plano de remediação, incluindo a substituição da tecnologia, conforme necessário.

***Observação**: Algumas práticas recomendadas nesta seção também estão incluídas como requisitos do PCI DSS para certas entidades. Por exemplo, aqueles que estão passando por uma avaliação completa do PCI DSS, prestadores de serviços que validam os requisitos adicionais "apenas para prestador de serviços" e entidades designadas que são obrigadas a validar de acordo com o Apêndice A3: Validação Complementar de Entidades Designadas.*

Cada entidade deve considerar a implementação dessas práticas recomendadas em seu ambiente, mesmo que a entidade não seja obrigada a validá-las (por exemplo, comerciantes em autoavaliação).

Consulte as *Melhores Práticas para Manter a Conformidade com o PCI DSS* na Biblioteca de documentos no site do PCI SSC para obter orientações adicionais.

6 Para os Assessores: Amostragem para as Avaliações do PCI DSS

A amostragem é uma opção para os assessores que realizam avaliações do PCI DSS para facilitar o processo de avaliação quando há um grande número de itens em uma população sendo testada.

Embora seja aceitável para um assessor obter amostras de itens semelhantes em uma população sendo testada como parte de sua revisão da conformidade do PCI DSS de uma entidade, não é aceitável para uma entidade aplicar os requisitos do PCI DSS a apenas uma amostra de seu ambiente (para exemplo, os requisitos para varreduras de vulnerabilidade trimestrais se aplicam a todos os componentes do sistema). Da mesma forma, não é aceitável que um assessor analise apenas uma amostra dos requisitos do PCI DSS para a conformidade.

Embora a amostragem permita que os assessores testem menos de 100% de uma determinada população de amostragem, os assessores devem sempre se esforçar para obter a revisão mais completa possível. Os assessores são incentivados a usar processos automatizados ou outros mecanismos se a população completa, independentemente do tamanho, puder ser testada de forma rápida e eficiente, com impacto mínimo nos recursos da entidade que está sendo avaliada. Onde os processos automatizados não estão disponíveis para testar 100% de uma população, a amostragem é uma abordagem igualmente aceitável.

Depois de considerar o escopo geral, a complexidade e a consistência do ambiente que está sendo avaliado e a natureza (automatizada ou manual) dos processos usados por uma entidade para atender a um requisito, o assessor pode selecionar independentemente amostras representativas das populações que estão sendo analisadas para avaliar a conformidade da entidade com os requisitos do PCI DSS. As amostras devem ser uma seleção representativa de todas as variantes da população e devem ser suficientemente grandes para fornecer ao assessor a garantia de que os controles são implementados conforme o esperado em toda a população. Ao testar o desempenho periódico de um requisito (por exemplo, semanal ou trimestralmente ou periodicamente), o assessor deve tentar selecionar uma amostra que represente todo o período coberto pela avaliação para que o assessor possa fazer um julgamento razoável de que o requisito foi cumprido durante todo o período de avaliação. Testar a mesma amostra de itens ano após ano pode permitir que variações desconhecidas nos itens não amostrados permaneçam não detectadas. Os assessores devem revalidar a lógica da amostragem para cada avaliação e considerar os conjuntos de amostras anteriores. Amostras diferentes devem ser selecionadas para cada avaliação.

A seleção apropriada da amostra depende do que está sendo considerado ao examinar os membros da amostra. Por exemplo, determinar a presença de antimalware em servidores sabidamente afetados por software malicioso pode levar à determinação da população de todos os servidores no ambiente, ou todos os servidores no ambiente que estão executando um determinado sistema operacional, ou todos os servidores que não são mainframes, etc. A seleção de uma amostra apropriada incluiria, então, representantes de TODOS os membros da população identificada, incluindo todos os servidores que executam o sistema operacional identificado, incluindo todas as versões, bem como servidores dentro da população que são usados para funções diferentes (servidor web, servidores de aplicativos, servidores de banco de dados, etc.).

No caso de um item de configuração específico estar sendo considerado, a população pode ser dividida apropriadamente e os grupos de amostra separados identificados. Por exemplo, uma amostra de todos os servidores pode não ser apropriada ao revisar uma definição de configuração do sistema operacional, em que diferentes sistemas operacionais estão presentes no ambiente. Nesse caso, as amostras de cada tipo de sistema operacional seriam apropriadas para identificar se a configuração foi definida de forma adequada para cada sistema

operacional. Cada conjunto de amostra deve incluir servidores representativos de cada tipo de sistema operacional, incluindo a versão, bem como funções representativas.

Outros exemplos de amostragem incluem seleções de pessoal com funções semelhantes ou variadas, com base no requisito que está sendo avaliado; por exemplo, uma amostra de administradores versus uma amostra de todos os funcionários.

O assessor deve usar julgamento profissional no planejamento, desempenho e avaliação da amostra para apoiar sua conclusão sobre se e como a entidade atendeu a um requisito. O objetivo do assessor na amostragem é obter evidências suficientes para ter uma base razoável para sua opinião. Ao selecionar amostras de forma independente, os assessores devem considerar o seguinte:

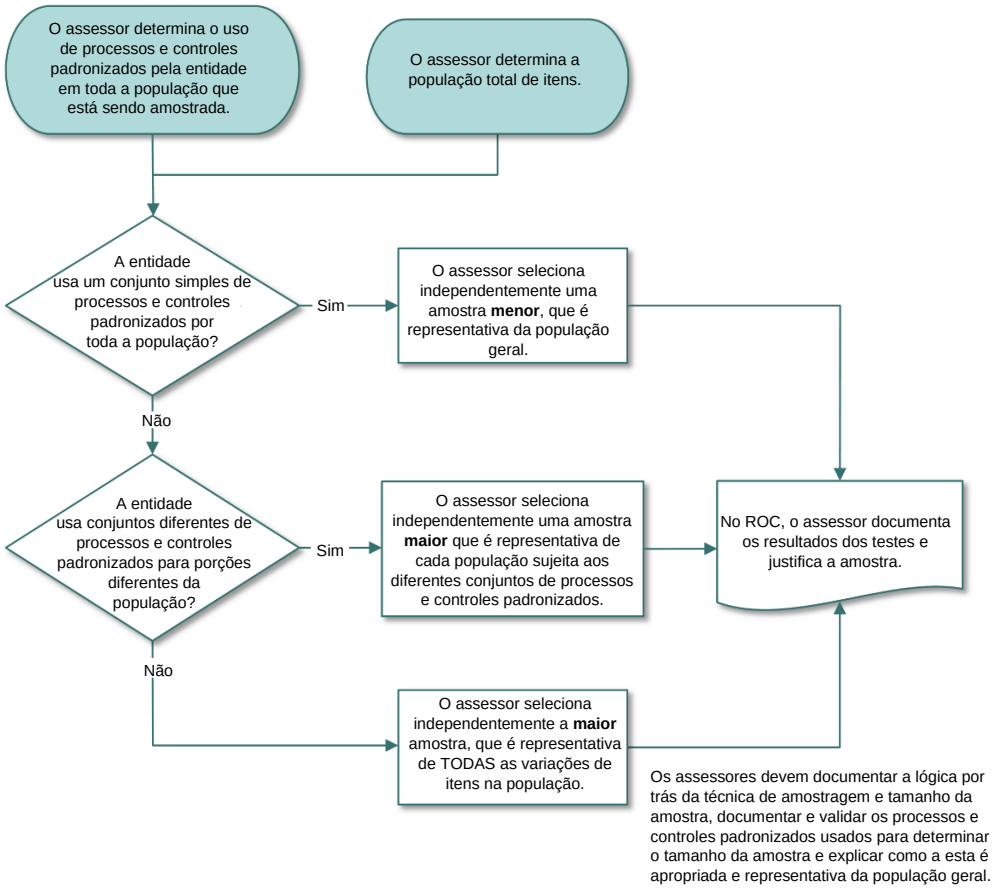
- O assessor deve selecionar a amostra da população completa sem influência da entidade avaliada.
- Se a entidade possui processos e controles padronizados implementados que garantem consistência e que são aplicados a cada item da população, a amostra pode ser menor do que se a entidade não tivesse processos/controles padronizados implementados. A amostra deve ser grande o suficiente para fornecer ao assessor uma garantia razoável de que os itens da população aderem aos processos padronizados que são aplicados a cada item da população. O assessor deve verificar se os controles padronizados estão implementados e funcionando de forma eficaz.
- Se a entidade tiver mais de um tipo de processo padronizado implementado (por exemplo, para diferentes tipos de instalações de negócios/componentes do sistema), a amostra deve incluir itens sujeitos a cada tipo de processo. Por exemplo, as populações podem ser divididas em subpopulações com base em características que podem impactar a consistência dos requisitos avaliados, como o uso de diferentes processos ou ferramentas. As amostras seriam então selecionadas de cada subpopulação.
- Se a entidade não tiver processos/controles padronizados do PCI DSS implementados e cada item da população for gerenciado por meio de processos não padronizados, a amostra deve ser maior para que o assessor tenha certeza de que os requisitos do PCI DSS são aplicados de forma adequada a cada item na população.
- As amostras de componentes do sistema devem incluir todos os tipos e combinações que estão sendo usados. Quando uma entidade tem mais de um CDE, as amostras devem incluir populações em todos os componentes de sistema dentro do escopo. Por exemplo, onde os aplicativos são amostrados, a amostra deve incluir todas as versões e plataformas para cada tipo de aplicativo.
- Os tamanhos das amostras devem ser sempre maiores que um, a menos que haja apenas um item na população dada, ou um controle automatizado seja usado quando o assessor tiver confirmado que o controle está funcionando conforme programado para cada população de amostra avaliada.
- Se o assessor depende de processos e controles padronizados implantados como base para a seleção de uma amostra, mas depois descobre durante o teste que os processos e controles padronizados não estão implantados ou não operam de forma eficaz, o assessor deve então aumentar o tamanho da amostra para tentar obter a garantia de que os requisitos do PCI DSS estão sendo atendidos.

Para cada instância em que a amostragem é usada, o assessor deve:

- Documentar a lógica por trás da técnica de amostragem e tamanho da amostra.
- Validar e documentar os processos e controles padronizados usados para determinar o tamanho da amostra.
- Explicar como a amostra é apropriada e representativa da população em geral.

A Figura 3 mostra as considerações para determinar o tamanho da amostra.

Figura 3. Considerações de Amostragem do PCI DSS



***Observação**: No PCI DSS v4.0, as referências específicas à amostragem foram removidas de todos os procedimentos de teste. Essas referências foram removidas porque mencionar a amostragem apenas em alguns procedimentos de teste pode ter implicado que a amostragem era obrigatória para esses procedimentos de teste (o que não era), ou que a amostragem só era permitida onde era especificamente mencionada. Os assessores devem selecionar amostras quando for apropriado para a população que está sendo testada e, conforme acima, tomar essas decisões após considerar o escopo geral e a complexidade de um ambiente.*

7 Descrição dos Prazos Usados nos Requisitos do PCI DSS

Certos requisitos do PCI DSS foram estabelecidos com prazos específicos para atividades que precisam ser realizadas de forma consistente por meio de um processo programado regularmente e repetível. A intenção é que a atividade seja realizada em um intervalo o mais próximo possível desse intervalo de tempo, sem excedê-lo. A entidade tem o poder de realizar uma atividade com mais frequência do que o especificado (por exemplo, realizar uma atividade mensalmente em que o requisito do PCI DSS especifica que seja realizada a cada três meses).

A Tabela 4 descreve a frequência para os diferentes períodos de tempo usados nos Requisitos do PCI DSS.

Tabela 4. Prazos dos Requisitos do PCI DSS

Prazos dos Requisitos do PCI DSS	Descrições e Exemplos
Diariamente	Todos os dias do ano (não somente os dias úteis).
Semanalmente	Pelo menos uma vez a cada sete dias.
Mensalmente	Pelo menos uma vez a cada 30 ou 31 dias, ou no enésimo dia do mês.
A cada três meses (“trimestralmente”)	Pelo menos uma vez a cada 90 ou 92 dias, ou no enésimo dia do trimestre.
A cada seis meses	Pelo menos uma vez a cada 180 ou 184 dias, ou no enésimo dia do semestre.
A cada 12 meses (“anualmente”)	Pelo menos uma vez a cada 365 (ou 366 para anos bissextos) dias ou na mesma data todo ano.
Periodicamente	A frequência de ocorrência fica a critério da entidade e é documentada e apoiada pela análise de risco da entidade. A entidade deve demonstrar que a frequência é apropriada para que a atividade seja eficaz e atenda à intenção do requisito.
Imediatamente	Sem atrasos. Em tempo real ou quase em tempo real.
Prontamente	Assim que razoavelmente possível.

Prazos dos Requisitos do PCI DSS	Descrições e Exemplos
Mudança significativa	Existem certos requisitos para os quais o desempenho é especificado mediante uma mudança significativa no ambiente de uma entidade. Embora o que constitui uma mudança significativa seja altamente dependente da configuração de um determinado ambiente, cada uma das seguintes atividades, no mínimo, tem impactos potenciais na segurança do CDE e deve ser considerada como uma mudança significativa no contexto relacionado aos requisitos de PCI DSS: • Novo hardware, software ou equipamento de rede adicionado ao CDE. • Qualquer substituição ou atualização importante de hardware e software no CDE. • Quaisquer alterações no fluxo ou armazenamento de dados da conta. • Quaisquer alterações nos limites do CDE e/ou no escopo da avaliação do PCI DSS. • Quaisquer alterações na infraestrutura de suporte subjacente do CDE (incluindo, mas não se limitando a, alterações nos serviços de diretório, servidores de tempo, registros e monitoramento). • Quaisquer alterações em fornecedores/prestadores de serviços terceirizados (ou serviços prestados) que oferecem suporte ao CDE ou atendem aos requisitos do PCI DSS em nome da entidade.

Para outros requisitos do PCI DSS, em que o padrão não define uma frequência mínima para atividades recorrentes, mas permite que o requisito seja atendido “periodicamente”, espera-se que a entidade defina a frequência apropriada para seus negócios. A frequência definida pela entidade deve ser apoiada pela política de segurança da entidade e pela análise de risco realizada de acordo com o Requisito 12.3.1 do PCI DSS. A entidade também deve ser capaz de demonstrar que a frequência por ela definida é apropriada para que a atividade seja eficaz e atenda à intenção do requisito.

Em ambos os casos, onde o PCI DSS especifica uma frequência necessária e onde o PCI DSS permite o desempenho "periódico", espera-se que a entidade tenha processos documentados e implementados para garantir que as atividades sejam realizadas dentro de um prazo razoável, incluindo pelo menos o seguinte:

- A entidade é prontamente notificada sempre que uma atividade não é realizada de acordo com seu cronograma definido,
- A entidade determina os eventos que levaram à perda de uma atividade programada,
- A entidade realiza a atividade o mais rápido possível depois que ela é perdida e volta ao cronograma ou estabelece um novo cronograma,
- A entidade produz documentação que mostra os elementos acima ocorridos.

Quando uma entidade tem os processos acima implementados para detectar e resolver quando uma atividade programada é perdida, uma abordagem razoável é permitida, o que significa que se uma atividade deve ser realizada pelo menos uma vez a cada três meses, a entidade não fica automaticamente fora de conformidade se a atividade for realizada tarde onde o processo documentado e implementado da entidade (conforme acima) foi seguido. No entanto, quando esse processo não está implementado e/ou a atividade não foi realizada de acordo com o cronograma devido à supervisão, má gestão ou falta de monitoramento, a entidade não atendeu ao requisito. Nesses casos, o requisito só

estará implementado quando a entidade 1) documentar (ou reconfirmar) o processo conforme acima para garantir que a atividade programada ocorra no prazo, 2) restabelecer o cronograma e 3) fornecer evidências de que a entidade executou a atividade programada pelo menos uma vez de acordo com sua programação.

***Observação**: Para uma avaliação inicial do PCI DSS (o que significa que uma entidade nunca passou por uma avaliação anterior), onde um requisito tem um prazo definido dentro do qual uma atividade deve ocorrer, não é necessário que a atividade tenha sido realizada para cada prazo durante o ano anterior, se o assessor verificar:*

- *A atividade foi realizada de acordo com o requisito aplicável dentro do período de tempo mais recente (por exemplo, o período de três ou seis meses mais recente), e*
- *A entidade documentou políticas e procedimentos para continuar a realizar a atividade dentro do prazo definido.*

Para os anos subsequentes após a avaliação inicial, a atividade deve ter sido realizada pelo menos uma vez dentro de cada período de tempo exigido. Por exemplo, uma atividade necessária a cada três meses deve ter sido realizada pelo menos quatro vezes durante o ano anterior em um intervalo que não exceda 90-92 dias.

8 Abordagens para Implementação e Validação do PCI DSS

Para oferecer suporte à flexibilidade em como os objetivos de segurança são atendidos, há duas abordagens para implementar e validar o PCI DSS. As entidades devem identificar a abordagem mais adequada para sua implementação de segurança e usar essa abordagem para validar os controles.

Abordagem Definida

Segue o método tradicional de implementação e validação do PCI DSS e usa os Requisitos e Procedimentos de Teste definidos no padrão. Na abordagem definida, a entidade implementa controles de segurança para atender aos requisitos declarados, e o assessor segue os procedimentos de teste definidos para verificar se os requisitos foram atendidos.

A abordagem definida oferece suporte a entidades com controles implementados que atendem aos requisitos do PCI DSS conforme declarado. Essa abordagem também pode ser adequada a entidades que desejam mais orientações sobre como atender aos objetivos de segurança, bem como entidades novas em segurança de informações ou PCI DSS.

Controles de Compensação

Como parte da abordagem definida, as entidades que não podem atender a um requisito do PCI DSS explicitamente conforme declarado devido a uma restrição técnica ou comercial legítima e documentada podem implementar outros, ou *compensar controles* que mitiguem suficientemente o risco associado ao requisito. Em uma base anual, quaisquer controles de compensação devem ser documentados pela entidade e revisados e validados pelo assessor e incluídos no envio do Relatório de Conformidade.

Observação: *Para obter mais detalhes, consulte o Apêndice B: Controles de Compensação e o Apêndice C: Planilha de Controles de Compensação.*

Abordagem Personalizada

Concentra-se no objetivo de cada requisito do PCI DSS,(se aplicável) permitindo que as entidades implementem controles para atender ao requisito declarado no objetivo da abordagem personalizada de uma forma que não siga estritamente o requisito definido. Como cada implementação personalizada será diferente, não há procedimentos de teste definidos; o assessor deve derivar procedimentos de teste que são apropriados para a implementação específica para validar se os controles implementados atendem ao objetivo declarado.

Observação: *Para obter mais detalhes, consulte o Apêndice D: Abordagem Personalizada e o Apêndice E: Modelos de Amostra para Apoiar a Abordagem Personalizada.*

A abordagem personalizada oferece suporte à inovação nas práticas de segurança, permitindo às entidades maior flexibilidade para mostrar como seus controles de segurança atuais atendem aos objetivos do PCI DSS. Essa abordagem é destinada a entidades maduras para riscos que demonstram uma abordagem de gerenciamento de risco robusta para a segurança, incluindo, mas não se limitando a, um departamento de gerenciamento de risco dedicado ou uma abordagem de gerenciamento de risco em toda a organização.

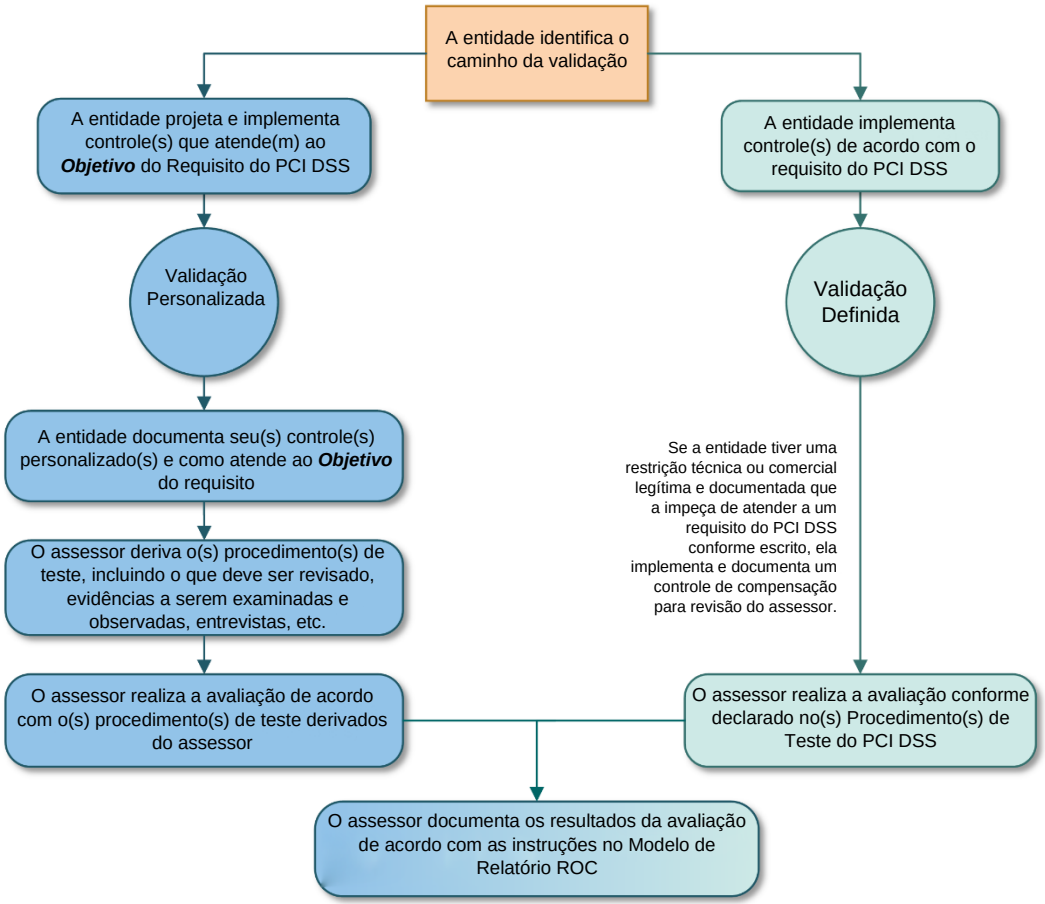
Espera-se que os controles implementados e validados usando a abordagem customizada atendam ou excedam a segurança fornecida pelo requisito na abordagem definida. O nível de documentação e esforço necessário para validar implementações personalizadas também será maior do que para a abordagem definida.

A maioria dos requisitos do PCI DSS pode ser atendida usando tanto a abordagem definida ou personalizada. Não obstante, vários requisitos não têm um Objetivo de Abordagem Personalizada declarado; a abordagem personalizada não é uma opção para esses requisitos.

As entidades podem usar tanto as abordagens definidas quanto as personalizadas em seu ambiente. Isso significa que uma entidade pode usar a abordagem definida para atender a alguns requisitos e usar a abordagem customizada para atender a outros requisitos. Significa também que uma entidade pode usar a abordagem definida para atender a um determinado requisito do PCI DSS para um componente de sistema ou em um ambiente, bem como usar a abordagem personalizada para atender ao mesmo requisito do PCI DSS para um componente de sistema diferente ou em um ambiente diferente. Dessa forma, uma avaliação do PCI DSS pode incluir procedimentos de teste definidos e personalizados.

A Figura 4 mostra as duas opções de validação para o PCI DSS v4.0.

Figura 4. Abordagens de Validação do PCI DSS



9 Proteção de Informações Sobre a Postura de Segurança de uma Entidade

Os processos relacionados a se tornar e manter um ambiente em conformidade com o PCI DSS resultam em muitos artefatos que uma entidade pode considerar confidenciais e pode querer proteger como tal, incluindo itens como os seguintes:

- O Relatório de Conformidade ou Questionário de Autoavaliação (o Atestado de Conformidade associado não é considerado confidencial e espera-se que os prestadores de serviços terceirizados (TPSPs) compartilhem seu AOC com os clientes).
- Diagramas de rede e diagramas de fluxo de dados da conta, e configurações e regras de segurança.
- Padrões de configuração de sistema.
- Métodos e protocolos de criptografia e gerenciamento de chaves.

As entidades devem revisar todos os artefatos relacionados aos controles de PCI DSS ou à avaliação e protegê-los de acordo com as políticas de segurança da entidade para este tipo de informação.

Os TPSPs são requeridos (Requisito 12.9 do PCI DSS) para apoiar seus clientes com o seguinte:

- Informações necessárias para que os clientes monitorem o status de conformidade do PCI DSS dos TPSPs (para permitir que o cliente cumpra o Requisito 12.8), e
- Evidência de que o TPSP está atendendo aos requisitos do PCI DSS aplicáveis onde os serviços do TPSP se destinam a atender ou facilitar o atendimento aos requisitos do PCI DSS de um cliente, ou onde esses serviços podem impactar a segurança do CDE de um cliente.

Esta seção não afeta ou nega a obrigação do TPSP de apoiar e fornecer informações aos seus clientes de acordo com o Requisito 12.9.

Para obter mais detalhes sobre as expectativas dos TPSPs e relacionamentos entre os TPSPs e clientes, consulte Uso de Prestadores de Serviços Terceirizados.

Proteção de Informações Confidenciais e Sensíveis por Empresas Assessoras de Segurança Qualificadas

Cada empresa Assessora de Segurança Qualificada (QSA) assina um contrato com o PCI SSC de que atenderá aos requisitos de qualificação para QSAs. A seção *Proteção de Informações Confidenciais e Sensíveis* desse documento inclui o seguinte:

> "A empresa QSA deve ter e aderir a um processo documentado para proteção de informações confidenciais e sigilosas. Isso deve incluir proteções físicas, eletrônicas e procedimentais adequadas, consistentes com as práticas aceitas pelo setor para proteger informações confidenciais e sensíveis contra quaisquer ameaças ou acesso não autorizado durante o armazenamento, processamento e/ou comunicação dessas informações.
>
> A Empresa QSA deve manter a privacidade e a confidencialidade das informações obtidas durante o desempenho de seus deveres e obrigações como Empresa QSA, a menos (e na medida em que) a divulgação seja exigida por autoridade legal."

10 Método de Teste para os Requisitos do PCI DSS

Os métodos de teste identificados nos procedimentos de teste para cada requisito descrevem as atividades esperadas a serem realizadas pelo assessor para determinar se a entidade atendeu ao requisito. A intenção por trás de cada método de teste é descrita a seguir:

- Examinar: O assessor 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.
- Observar: O assessor 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.
- Entrevistar: O assessor 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 têm como objetivo permitir que a entidade avaliada demonstre como atendeu a um requisito. Eles também fornecem à entidade avaliada e ao assessor um entendimento comum das atividades de avaliação a serem realizadas. 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 de cada entidade. Ao documentar os resultados da avaliação, o assessor identifica as atividades de teste realizadas e o resultado de cada atividade.

11 Instruções e Conteúdo para Relatório de Conformidade

As instruções e o conteúdo do Relatório de Conformidade (ROC) são fornecidos *no Modelo de Relatório de Conformidade (ROC) do PCI DSS*.

O modelo de Relatório de Conformidade (ROC) do PCI DSS deve ser usado como modelo para a criação de um relatório de conformidade do PCI DSS.

Se alguma entidade é obrigada a cumprir ou validar sua conformidade com o PCI DSS, fica a critério das organizações que gerenciam programas de conformidade (como bandeiras de pagamento e adquirentes). As entidades devem entrar em contato com as organizações de interesse para determinar quaisquer requisitos e instruções de relatórios.

12 Processo de Avaliação do PCI DSS

O processo de avaliação do PCI DSS inclui as seguintes etapas de alto nível:[5]

1. Confirmar o escopo da avaliação do PCI DSS
2. Realizar a avaliação do PCI DSS do ambiente.
3. Preencher o relatório aplicável para a avaliação de acordo com as orientações e instruções do PCI DSS.
4. Preencher o Atestado de Conformidade para prestadores de serviços ou comerciantes, conforme aplicável, em sua totalidade. Os Atestados Oficiais de Conformidade estão disponíveis apenas no site do PCI SSC.
5. Envie a documentação do PCI SSC aplicável e o Atestado de Conformidade, juntamente com qualquer outra documentação solicitada - como relatórios de varredura ASV - para a organização solicitante (aquelas que gerenciam programas de conformidade, como bandeiras de pagamento e adquirentes (para comerciantes), ou outros solicitantes (para prestadores de serviços)).
6. Se necessário, execute a correção para atender aos requisitos que não estão implementados e forneça um relatório atualizado.

Observação: *Os requisitos do PCI DSS não são considerados implementados se os controles ainda não foram implementados ou estão programados para serem concluídos em uma data futura. Depois que qualquer item em aberto ou não implementado for tratado pela entidade, o assessor fará uma reavaliação para validar se a remediação foi concluída e se todos os requisitos foram atendidos. Consulte os seguintes recursos (disponíveis no site do PCI SSC) para documentar a avaliação do PCI DSS:*

- *Para obter instruções sobre como preencher relatórios de conformidade (ROC), consulte o modelo de relatório de conformidade (ROC) do PCI DSS.*
- *Para obter instruções sobre como preencher os questionários de autoavaliação (SAQ), consulte as Instruções e diretrizes para SAQs do PCI DSS.*
- *Para obter instruções sobre como enviar relatórios de validação de conformidade do PCI DSS, consulte o Atestado de Conformidade do PCI DSS.*

[5] O processo de avaliação do PCI DSS e as funções e responsabilidades para a conclusão de cada etapa variam dependendo do tipo de avaliação e dos programas de conformidade, que são gerenciados por bandeiras de pagamento e adquirentes.

13 Referências Adicionais

A Tabela 5 lista as organizações externas referenciadas nos requisitos do PCI DSS ou nas orientações relacionadas. Essas organizações externas e suas referências são fornecidas apenas como informação e não substituem ou estendem qualquer requisito do PCI DSS.

Tabela 5. Organizações Externas Referenciadas nos Requisitos do PCI DSS

Referência	Nome Completo	Fonte
ANSI	American National Standards Institute	www.ansi.org
CIS	Center for Internet Security	www.cisecurity.org
CSA	Cloud Security Alliance	www.csa.org
ENISA	European Union Agency for Cybersecurity (formerly European Network and Information Security Agency)	www.enisa.europa.eu
FIDO Alliance	The FIDO Alliance	www.fidoalliance.org
ISO	International Organization for Standardization	www.iso.org
NCSC	The UK National Cyber Security Centre	www.ncsc.gov.uk
NIST	National Institute of Standards and Technology	www.nist.gov
OWASP	Open Web Application Security Project	www.owasp.org
SAFEcode	Software Assurance Forum for Excellence in Code	www.safecode.org

14 Versões do PCI DSS

Na data de publicação deste documento, o PCI DSS v3.2.1 é válido até 31 de março de 2024, após o qual será retirado. Todas as validações do PCI DSS após esta data devem ser para o PCI DSS 4.0 ou posterior.

O PCI DSS versão 3.2.1 ou 4.0 pode ser usado para avaliações entre março de 2022 e 31 de março de 2024.

A Tabela 6 resume as versões do PCI DSS e suas datas relevantes.[6]

Tabela 6. Versões do PCI DSS

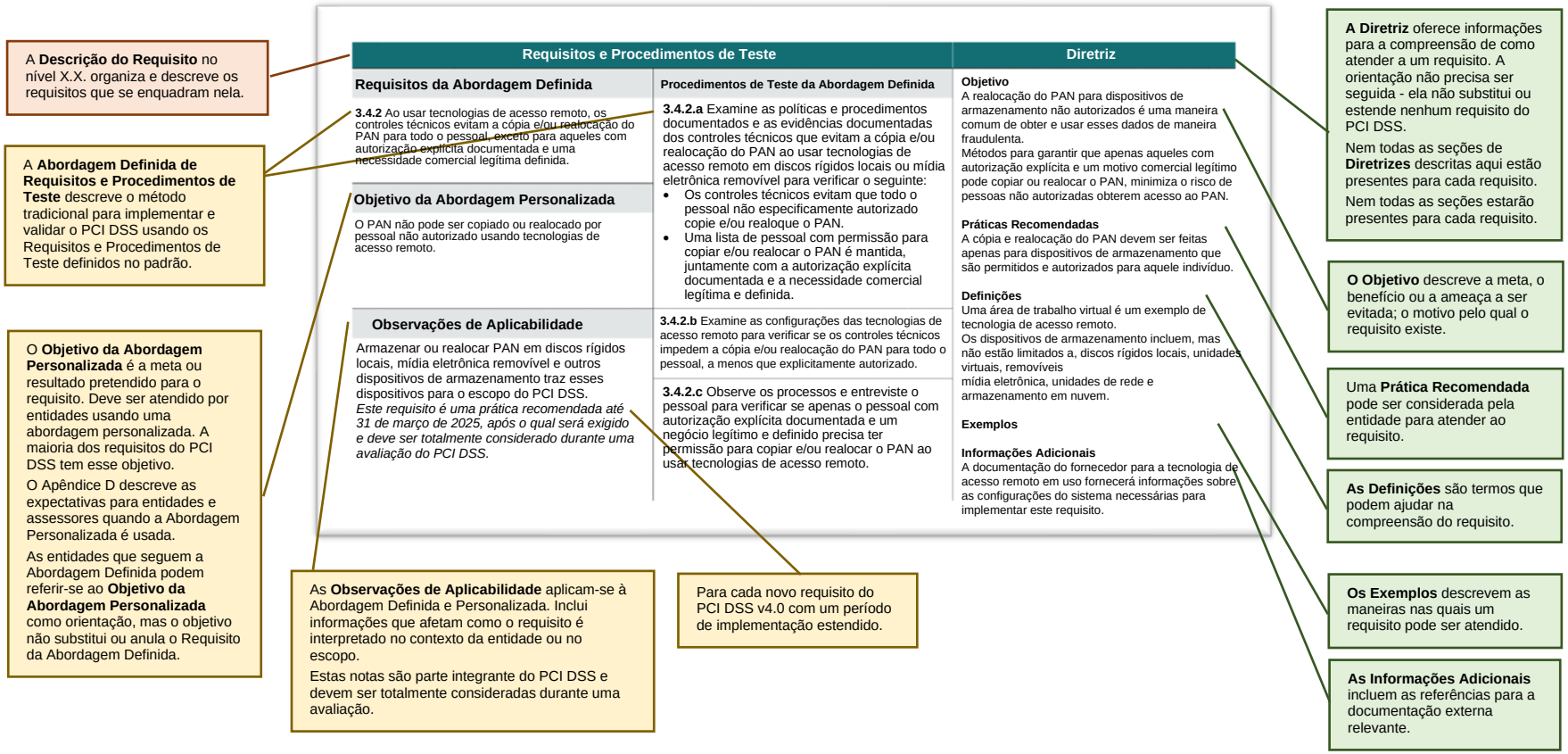
Versão	Publicado	Retirado
PCI DSS v4.0 (este documento)	Março de 2022	A ser determinado
PCI DSS v3.2.1	Maio de 2018	31 de Março, 2024

[6] Sujeito a alterações no lançamento de uma nova versão do PCI DSS.

15 Requisitos e Processos de Teste Detalhados do PCI DSS

A Figura 5 descreve os cabeçalhos das colunas e o conteúdo dos requisitos do PCI DSS.

Figura 5. Entendendo as Partes do Requisito



Requisitos Adicionais Apenas para Prestadores de Serviços

Alguns requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. Estes são identificados no requisito como "*Requisito adicional apenas para prestadores de serviços"* e aplicam-se em adição a todos os outros requisitos aplicáveis. Quando a entidade que está sendo avaliada é um comerciante e um prestador de serviços, os requisitos indicados como "*Requisito adicional apenas para prestadores de serviços"* se aplicam à parte do prestador de serviços dos negócios da entidade. Requisitos identificados com "*Requisito adicional apenas para prestadores de serviços"* também são recomendados como boas práticas para consideração por todas as entidades.

Apêndices com Requisitos Adicionais do PCI DSS para Diferentes Tipos de Entidades

Além dos 12 requisitos principais, o Apêndice A do PCI DSS contém requisitos adicionais do PCI DSS para diferentes tipos de entidades. As seções dentro do Apêndice A incluem:

- Apêndice A1: Requisitos Adicionais do PCI DSS para Prestadores de serviços Multilocatários.
- Apêndice A2: Requisitos Adicionais do PCI DSS para Entidades que usam SSL/TLS Antigo para Conexões de Terminal POS POI com Cartão Presente.
- Apêndice A3: Validação Complementar de Entidades Designadas (DESV).

Construir e Manter uma Rede e Sistemas Seguros

Requisito 1: Instalar e Manter Controles de Segurança de Rede

Seções	
1.1	Os processos e mecanismos para instalar e manter os controles de segurança da rede são definidos e compreendidos.
1.2	Os controles de segurança de rede (NSCs) são configurados e mantidos.
1.3	O acesso à rede de e para o ambiente de dados do titular do cartão é restrito.
1.4	As conexões de rede entre redes confiáveis e não confiáveis são controladas.
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.

Visão Geral

Os controles de segurança de rede (NSCs), como firewalls e outras tecnologias de segurança de rede, são pontos de aplicação de política de rede que normalmente controlam o tráfego de rede entre dois ou mais segmentos de rede físicos ou lógicos (ou sub-redes) com base em *políticas* ou *regras* predefinidas.

Os NSCs examinam todo o tráfego de rede que entra (ingresso) e sai (egresso) de um segmento e decidem, com base nas políticas definidas, se o tráfego de rede pode passar ou se deve ser rejeitado. Normalmente, os NSCs são colocados entre ambientes com diferentes necessidades de segurança ou níveis de confiança; todavia, em alguns ambientes, os NSCs controlam o tráfego para dispositivos individuais, independentemente dos limites de confiança. A aplicação da política geralmente ocorre na camada 3 do modelo OSI, mas os dados presentes nas camadas superiores também são frequentemente usados para determinar as decisões de política.

Tradicionalmente, essa função é fornecida por firewalls físicos; entretanto, agora essa funcionalidade pode ser fornecida por dispositivos virtuais, controles de acesso à nuvem, sistemas de virtualização/contêiner e outra tecnologia de rede definida por software.

Os NSCs são usados para controlar o tráfego dentro das redes da própria entidade - por exemplo, entre áreas altamente e menos sensíveis - e também para proteger os recursos da entidade da exposição a redes não confiáveis. O ambiente de dados do titular do cartão (CDE) é um exemplo de uma área mais sensível dentro da rede de uma entidade. Frequentemente, caminhos aparentemente insignificantes de e para redes não confiáveis podem fornecer caminhos desprotegidos para sistemas confidenciais. Os NSCs fornecem um mecanismo de proteção fundamental para qualquer rede de computadores.

Exemplos comuns de redes não confiáveis incluem a Internet, conexões dedicadas, como canais de comunicação empresa-a-empresa, redes wireless, redes de operadoras (como celulares), redes de terceiros e outras fontes fora da capacidade de controle da entidade. Ademais, as redes não confiáveis também incluem as redes corporativas que são consideradas fora do escopo do PCI DSS, porque não são avaliadas e, portanto, devem ser tratadas como não confiáveis porque a existência de controles de segurança não foi verificada. Embora uma entidade possa considerar uma rede interna confiável do ponto de vista da infraestrutura, se uma rede estiver fora do escopo do PCI DSS, essa rede deve ser considerada não confiável para o PCI DSS.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
1.1 Os processos e mecanismos para instalar e manter os controles de segurança da rede são definidos e compreendidos.		
Requisitos da Abordagem Definida **1.1.1** Todas as políticas e processos operacionais identificados no Requisito 1 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 1 são definidos, compreendidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **1.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 1 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 1.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 1. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 1, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esses motivos, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
1.1.2 As funções e responsabilidades para a execução de atividades no Requisito 1 são documentadas, atribuídas e compreendidas.	**1.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 1 estão documentadas e atribuídas.	
	1.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 1 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 1 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
1.2 Os controles de segurança de rede (NSCs) são configurados e mantidos.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
1.2.1 Os padrões de configuração para conjuntos de regras do NSC estão: • Definidas. • Implementadas. • Mantidas.	**1.2.1.a** Examine os padrões de configuração para conjuntos de regras do NSC para verificar se os padrões estão de acordo com todos os elementos especificados neste requisito.	A implementação desses padrões de configuração resulta no NSC sendo configurado e gerenciado para executar adequadamente sua função de segurança (frequentemente chamada de conjunto de regras). **Práticas Recomendadas** Esses padrões geralmente definem os requisitos para protocolos aceitáveis, portas que podem ser usadas e requisitos de configuração específicos que são aceitáveis. Os padrões de configuração também podem delinear o que a entidade considera não aceitável ou não permitido em sua rede. **Definições** Os NSCs são os componentes principais de uma arquitetura de rede. Mais comumente, os NSCs são usados nos limites do CDE para controlar o tráfego de rede que flui de entrada e saída do CDE. Os padrões de configuração descrevem os requisitos mínimos de uma entidade para a configuração de seus NSCs **Exemplos** Exemplos de NSCs cobertos por esses padrões de configuração incluem, mas não estão limitados a, firewalls, roteadores configurados com listas de controle de acesso e redes virtuais em nuvem.
Objetivo da Abordagem Personalizada	**1.2.1.b** Examine as definições de configuração dos conjuntos de regras do NSC para verificar se os conjuntos de regras são implementados de acordo com os padrões de configuração.	
A maneira como os NSCs são configurados e operam é definida e aplicada de forma consistente.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Práticas Recomendadas**
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.	**1.2.2.a** Examine os procedimentos documentados para verificar se as mudanças nas conexões de rede e configurações dos NSCs estão incluídas no processo formal de controle de mudanças de acordo com o Requisito 6.5.1.	As mudanças devem ser aprovadas por indivíduos com autoridade e conhecimento apropriados para entender o impacto da mudança. A verificação deve fornecer garantia razoável de que a mudança não afetou adversamente a segurança da rede e que o desempenho da mudança foi o esperado. A fim de evitar ter que resolver problemas de segurança introduzidos por uma mudança, todas as mudanças devem ser aprovadas antes de serem implementadas e verificadas após a mudança ser implementada. Depois de aprovada e verificada, a documentação da rede deve ser atualizada para incluir as mudanças para evitar inconsistências entre a documentação da rede e a configuração real.
	1.2.2.b Examine as definições de configuração de rede para identificar as mudanças feitas nas conexões de rede. Entreviste a equipe responsável e examine os registros de controle de mudanças para verificar se as mudanças identificadas nas conexões de rede foram aprovadas e gerenciadas de acordo com o Requisito 6.5.1.	
Objetivo da Abordagem Personalizada	**1.2.2.c** Examine as definições de configuração de rede para identificar as mudanças feitas nas configurações dos NSCs. Entreviste a equipe responsável e examine os registros de controle de mudanças para verificar se as mudanças identificadas nas configurações dos NSCs foram aprovadas e gerenciadas de acordo com o Requisito 6.5.1.	
As mudanças nas conexões de rede e nos NSCs não podem resultar em configuração incorreta, implementação de serviços inseguros ou conexões de rede não autorizadas.		
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 como ele executa sua função de segurança.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Manter um(s) diagrama(s) de rede preciso(s) atualizado(s) evita que as conexões e dispositivos de rede sejam negligenciados e, inadvertidamente, deixados sem segurança e vulneráveis a comprometimento. Um(s) diagrama(s) de rede devidamente mantido(s) ajuda(m) uma organização a verificar seu escopo do PCI DSS, identificando os sistemas que se conectam de e para o CDE. **Práticas Recomendadas** Todas as conexões de e para o CDE devem ser identificadas, incluindo sistemas que fornecem serviços de segurança, gerenciamento ou manutenção para os componentes do sistema CDE. As entidades devem considerar a inclusão do seguinte em seus diagramas de rede: • Todos os locais, incluindo locais de varejo, centros de dados, locais corporativos, provedores de nuvem, etc. • Identificação clara de todos os segmentos de rede. • Todos os controles de segurança que fornecem segmentação, incluindo identificadores exclusivos para cada controle (por exemplo, nome do controle, marca, modelo e versão). • Todos os componentes de sistema no escopo, incluindo NSCs, firewalls de aplicativos da web, soluções antimalware, soluções de gerenciamento de mudanças, IDS/IPS, sistemas de agregação de registro, terminais de pagamento, aplicativos de pagamento, HSMs, etc. • Identificação clara de quaisquer áreas fora do escopo no diagrama por meio de uma caixa sombreada ou outro mecanismo.
1.2.3 Um(s) diagrama(s) de rede preciso é mantido, mostrando todas as conexões entre o CDE e outras redes, incluindo quaisquer wireless.	**1.2.3.a** Examine o(s) diagrama(s) e as configurações de rede para verificar se existe(m) um(s) diagrama(s) de rede preciso(s) de acordo com todos os elementos especificados neste requisito.	
	1.2.3.b Examine a documentação e entreviste o pessoal responsável para verificar se o(s) diagrama(s) de rede são precisos e atualizados quando há mudanças no ambiente.	
Objetivo da Abordagem Personalizada		
Uma representação dos limites entre o CDE, todas as redes confiáveis e todas as redes não confiáveis é mantida e está disponível.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Um(s) diagrama(s) de rede atual(is) ou outra solução técnica ou topológica que identifique as conexões e dispositivos de rede podem ser usados para atender a esse requisito.		• Data da última atualização e nomes das pessoas que fizeram e aprovaram as atualizações. • Uma legenda ou chave para explicar o diagrama. Os diagramas devem ser atualizados por pessoal autorizado para garantir que continuem a fornecer uma descrição precisa da rede.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
1.2.4 Um(s) diagrama(s) de fluxo de dados preciso é mantido e atende ao seguinte: • Mostra todos os fluxos de dados da conta em sistemas e redes. • Atualizado conforme necessário mediante mudanças no ambiente.	**1.2.4.a** Examine o(s) diagrama(s) de fluxo de dados e entreviste o pessoal para verificar se o(s) diagrama(s) mostram todos os fluxos de dados da conta de acordo com todos os elementos especificados neste requisito.	Um diagrama de fluxo de dados atualizado e prontamente disponível ajuda uma organização a entender e controlar o escopo de seu ambiente, mostrando como os dados da conta fluem através das redes e entre sistemas e dispositivos individuais. Manter um(s) diagrama(s) de fluxo de dados atualizado(s) evita que os dados da conta sejam ignorados e deixados sem segurança inadvertidamente.
Objetivo da Abordagem Personalizada	**1.2.4.b** Examine a documentação e entreviste o pessoal responsável para verificar se o(s) diagrama(s) de fluxo de dados são precisos e atualizados quando há mudanças no ambiente.	**Práticas Recomendadas** O diagrama de fluxo de dados deve incluir todos os pontos de conexão onde os dados da conta são recebidos e enviados para fora da rede, incluindo conexões para redes públicas abertas, fluxos de processamento de aplicativos, armazenamento, transmissões entre sistemas e redes e backups de arquivos. O diagrama de fluxo de dados deve ser adicional ao diagrama de rede e deve se reconciliar e aumentar o diagrama de rede. Como prática recomendada, as entidades podem considerar a inclusão do seguinte em seus diagramas de fluxo de dados: • Todos os fluxos de processamento de dados da conta, incluindo autorização, captura, liquidação, estorno e reembolsos. • Todos os canais de aceitação distintos, incluindo cartão presente, cartão não presente e comércio eletrônico. • Todos os tipos de recebimento ou transmissão de dados, incluindo qualquer mídia em papel/cópia impressa. • O fluxo de dados da conta desde o ponto em que entra no ambiente, até sua disposição final. *(continua na página a seguir)*
Uma representação de todas as transmissões de dados da conta entre os componentes de sistema e entre os segmentos da rede é mantida e está disponível.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Um(s) diagrama(s) de fluxo de dados ou outra solução técnica ou topológica que identifica fluxos de dados da conta em sistemas e redes podem ser usados para atender a esse requisito.		• Onde os dados da conta são transmitidos e processados, onde são armazenados e se o armazenamento é de curto ou longo prazo. • A origem de todos os dados da conta recebidos (por exemplo, clientes, terceiros, etc.) e quaisquer entidades com as quais os dados da conta são compartilhados. • Data da última atualização e nomes das pessoas que fizeram e aprovaram as atualizações.
Requisitos da Abordagem Definida **1.2.5** Todos os serviços, protocolos e portas permitidas são identificados, aprovados e têm uma necessidade comercial definida. **Objetivo da Abordagem Personalizada** O tráfego de rede não autorizado (serviços, protocolos ou pacotes destinados a portas específicas) não pode entrar ou sair da rede.	**Procedimentos de Teste da Abordagem Definida** **1.2.5.a** Examine a documentação para verificar se existe uma lista de todos os serviços, protocolos e portas permitidos, incluindo justificativa comercial e aprovação para cada um. **1.2.5.b** Examine as definições de configuração dos NSCs para verificar se apenas serviços, protocolos e portas aprovados estão em uso.	**Objetivo** Os comprometimentos geralmente acontecem devido a serviços não utilizados ou inseguros (por exemplo, telnet e FTP), protocolos e portas, uma vez que podem levar à abertura de pontos de acesso desnecessários no CDE. Além disso, os serviços, protocolos e portas que estão habilitados, mas não em uso, costumam ser esquecidos e deixados sem segurança e sem atualização. Ao identificar os serviços, protocolos e portas necessários para os negócios, as entidades podem garantir que todos os outros serviços, protocolos e portas sejam desabilitados ou removidos. **Práticas Recomendadas** O risco de segurança associado a cada serviço, protocolo e porta permitida deve ser compreendido. As aprovações devem ser concedidas por pessoal independente daqueles que gerenciam a configuração. O pessoal de aprovação deve possuir conhecimento e responsabilidade apropriados para tomar decisões de aprovação.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Os comprometimentos tiram proveito de configurações de rede inseguras.
Práticas Recomendadas
Se serviços, protocolos ou portas inseguros forem necessários para os negócios, o risco representado por esses serviços, protocolos e portas deve ser claramente compreendido e aceito pela organização, o uso do serviço, protocolo ou porta deve ser justificado e os recursos de segurança que reduzem o risco de usar esses serviços, protocolos e portas devem ser definidos e implementados pela entidade.
Informações Adicionais
Para obter orientação sobre serviços, protocolos ou portas consideradas inseguras, consulte os padrões e orientações da indústria (por exemplo, do NIST, ENISA, OWASP).</td></tr>
<tr><td rowspan="2">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.</td><td>1.2.6.a Examine a documentação que identifica todos os serviços, protocolos e portas inseguros em uso para verificar se, para cada um, os recursos de segurança estão definidos para reduzir o risco.</td></tr>
<tr><td>1.2.6.b Examine as definições de configuração dos NSCs para verificar se os recursos de segurança definidos são implementados para cada serviço, protocolo e porta inseguros identificados.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada</td><td></td></tr>
<tr><td>Os riscos específicos associados ao uso de serviços, protocolos e portas inseguros são compreendidos, avaliados e adequadamente mitigados.</td><td></td><td></td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
1.2.7 As configurações dos NSCs são revisadas pelo menos uma vez a cada seis meses para confirmar que são relevantes e eficazes.	**1.2.7.a** Examine a documentação para verificar se os procedimentos são definidos para revisar as configurações dos NSCs pelo menos uma vez a cada seis meses.	**Objetivo** Tal revisão dá à organização a oportunidade de limpar quaisquer regras e configurações desnecessárias, desatualizadas ou incorretas que possam ser utilizadas por uma pessoa não autorizada. Ademais, garante que todas as regras e configurações permitam apenas serviços, protocolos e portas autorizados que correspondam às justificativas de negócios documentadas. **Práticas Recomendadas** Essa revisão, que pode ser implementada usando métodos manuais, automatizados ou baseados em sistema, tem como objetivo confirmar se as configurações que gerenciam as regras de tráfego, o que é permitido dentro e fora da rede, correspondem às configurações aprovadas. A revisão deve fornecer a confirmação de que todo o acesso permitido tem um motivo comercial justificado. Quaisquer discrepâncias ou incertezas sobre uma regra ou configuração devem ser escaladas para resolução. Embora esse requisito especifique que essa revisão ocorra pelo menos uma vez a cada seis meses, as organizações com um alto volume de alterações em suas configurações de rede podem considerar a realização de revisões com mais frequência para garantir que as configurações continuem atendendo às necessidades da empresa.
	1.2.7.b Examine a documentação das revisões das configurações dos NSCs e entreviste o pessoal responsável para verificar se as revisões ocorrem pelo menos uma vez a cada seis meses.	
Objetivo da Abordagem Personalizada	**1.2.7.c** Examine as configurações dos NSCs para verificar se as configurações identificadas como não sendo mais suportadas por uma justificativa de negócios foram removidas ou atualizadas.	
As configurações do NSC que permitem ou restringem o acesso a redes confiáveis são verificadas periodicamente para garantir que apenas conexões autorizadas com uma justificativa comercial atual sejam permitidas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **1.2.8** Os arquivos de configuração para os NSCs são: • Protegidos contra acesso não autorizado. • Mantidos consistentes com as configurações de rede ativas. **Objetivo da Abordagem Personalizada** Os NSCs não podem ser definidos ou modificados usando objetos de configuração não confiáveis (incluindo arquivos). **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.	**Procedimentos de Teste da Abordagem Definida** **1.2.8** Examine os arquivos de configuração dos NSCs para verificar se estão de acordo com todos os elementos especificados neste requisito.	**Objetivo** Para evitar que configurações não autorizadas sejam aplicadas à rede, os arquivos armazenados com configurações de controles de rede precisam ser mantidos atualizados e protegidos contra mudanças não autorizadas. Manter as informações de configuração atualizadas e seguras garante que as configurações corretas para os NSCs sejam aplicadas sempre que a configuração for executada. **Exemplos** Se a configuração segura de um roteador for armazenada em memória não volátil, quando esse roteador for reiniciado ou reinicializado, esses controles devem garantir que sua configuração segura seja restabelecida.

Requisitos e Procedimentos de Teste		Diretriz
1.3 O acesso à rede de e para o ambiente de dados do titular do cartão é restrito.		
Requisitos da Abordagem Definida **1.3.1** O tráfego de entrada para o CDE é restrito da seguinte forma: • Apenas para o tráfego que é necessário. • Todos os demais tráfegos são especificamente negados. **Objetivo da Abordagem Personalizada** O tráfego não autorizado não pode entrar no CDE.	**Procedimentos de Teste da Abordagem Definida** **1.3.1.a** Examine os padrões de configuração dos NSCs para verificar se eles definem a restrição do tráfego de entrada para o CDE de acordo com todos os elementos especificados neste requisito. **1.3.1.b** Examine as configurações dos NSCs para verificar se o tráfego de entrada para o CDE é restrito de acordo com todos os elementos especificados neste requisito.	**Objetivo** Este requisito visa evitar que indivíduos mal-intencionados acessem a rede da entidade por meio de endereços IP não autorizados ou usem serviços, protocolos ou portas de maneira não autorizada. **Práticas Recomendadas** Todo o tráfego de entrada para o CDE, independentemente de sua origem, deve ser avaliado para garantir que segue as regras estabelecidas e autorizadas. As conexões devem ser inspecionadas para garantir que o tráfego seja restrito apenas às comunicações autorizadas - por exemplo, restringindo endereços e portas de origem/destino e bloqueando o conteúdo. **Exemplos** Implementar uma regra que nega todo o tráfego de entrada e saída que não seja especificamente necessário - por exemplo, usando um "negar tudo" explícito ou negar implícito após a declaração de permissão - ajuda a evitar furos inadvertidos que permitiriam tráfego não intencional e potencialmente prejudicial.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
1.3.2 O tráfego de saída do CDE é restrito da seguinte forma: • Apenas para o tráfego que é necessário. • Todos os demais tráfegos são especificamente negados.	**1.3.2.a** Examine os padrões de configuração dos NSCs para verificar se eles definem a restrição do tráfego de saída do CDE de acordo com todos os elementos especificados neste requisito.	Este requisito visa evitar que indivíduos mal-intencionados e componentes de sistema comprometidos dentro da rede da entidade se comuniquem com um host externo não confiável. **Práticas Recomendadas** Todo o tráfego que sai do CDE, independentemente do destino, deve ser avaliado para garantir que segue as regras estabelecidas e autorizadas. As conexões devem ser inspecionadas para restringir o tráfego apenas às comunicações autorizadas - por exemplo, restringindo endereços e portas de origem/destino e bloqueando o conteúdo. **Exemplos** Implementar uma regra que nega todo o tráfego de entrada e saída que não seja especificamente necessário - por exemplo, usando um "negar tudo" explícito ou negar implícito após a declaração de permissão - ajuda a evitar furos inadvertidos que permitiriam tráfego não intencional e potencialmente prejudicial.
Objetivo da Abordagem Personalizada	**1.3.2.b** Examine as configurações dos NSCs para verificar se o tráfego de saída do CDE é restrito de acordo com todos os elementos especificados neste requisito.	
O tráfego não autorizado não pode sair do CDE.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
1.3.3 Os NSCs são instalados entre todas as redes wireless e o CDE, independentemente de a rede wireless ser um CDE, de modo que: • Todo o tráfego wireless de redes wireless para o CDE é negado por padrão. • Somente o tráfego wireless com uma finalidade comercial autorizada é permitido no CDE.	**1.3.3** Examine as definições de configuração e diagramas de rede para verificar se os NSCs são implementados entre todas as redes wireless e o CDE, de acordo com todos os elementos especificados neste requisito.	A implementação e exploração conhecidas (ou desconhecidas) de tecnologia wireless dentro de uma rede é um caminho comum para indivíduos mal-intencionados obterem acesso à rede e aos dados da conta. Se um dispositivo ou rede wireless for instalado sem o conhecimento da entidade, um indivíduo mal-intencionado pode facilmente e "invisivelmente" entrar na rede. Se os NSCs não restringirem o acesso de redes wireless ao CDE, indivíduos mal-intencionados que ganham acesso não autorizado à rede wireless podem se conectar facilmente ao CDE e comprometer as informações da conta.
Objetivo da Abordagem Personalizada		
O tráfego não autorizado não pode ultrapassar os limites da rede entre quaisquer redes wireless e ambientes cabeados no CDE.		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td colspan="3">1.4 As conexões de rede entre redes confiáveis e não confiáveis são controladas.</td></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
A implementação do NSCs em cada conexão que entra e sai de redes confiáveis permite que a entidade monitore e controle o acesso e minimiza as chances de um indivíduo mal-intencionado obter acesso à rede interna por meio de uma conexão desprotegida.
Exemplos
Uma entidade pode implementar uma DMZ, que é uma parte da rede que gerencia conexões entre uma rede não confiável (para exemplos de redes não confiáveis, consulte a Visão Geral do Requisito 1) e serviços que uma organização precisa disponibilizar ao público, como um servidor web. Observe que se a DMZ de uma entidade processa ou transmite dados da conta (por exemplo, site de comércio eletrônico), também é considerado um CDE.</td></tr>
<tr><td>1.4.1 Os NSCs são implementados entre redes confiáveis e não confiáveis.</td><td>1.4.1.a Examine os padrões de configuração e diagramas de rede para verificar se os NSCs são definidos entre redes confiáveis e não confiáveis.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
O tráfego não autorizado não pode ultrapassar os limites da rede entre redes confiáveis e não confiáveis.</td><td>1.4.1.b Examine as configurações de rede para verificar se os NSCs estão implementados entre redes confiáveis e não confiáveis, de acordo com os padrões de configuração documentados e diagramas de rede.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **1.4.2** O tráfego de entrada de redes não confiáveis para redes confiáveis é restrito a: • Comunicações com componentes de sistema autorizados a fornecer serviços, protocolos e portas acessíveis ao público. • Respostas com estado para comunicações iniciadas por componentes do sistema em uma rede confiável. • Todos os demais tráfegos são negados. **Objetivo da Abordagem Personalizada** Somente o tráfego autorizado ou que seja uma resposta a um componente de sistema na rede confiável pode entrar em uma rede confiável a partir de uma rede não confiável. **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.	**Procedimentos de Teste da Abordagem Definida** **1.4.2** Examine a documentação do fornecedor e as configurações dos NSCs para verificar se o tráfego de entrada de redes não confiáveis para redes confiáveis é restrito de acordo com todos os elementos especificados neste requisito.	**Objetivo** Garantir que o acesso público a um componente de sistema seja especificamente autorizado reduz o risco de os componentes de sistema serem desnecessariamente expostos a redes não confiáveis. **Práticas Recomendadas** Os componentes de sistema que fornecem serviços acessíveis ao público, como e-mail, web e servidores DNS, são os mais vulneráveis a ameaças originadas de redes não confiáveis. Idealmente, esses sistemas são colocados em uma rede confiável personalizada que é voltada para o público (por exemplo, uma DMZ), mas que é separada por meio de NSCs de sistemas internos mais sensíveis, o que ajuda a proteger o resto da rede no caso de esses sistemas acessíveis externamente serem comprometidos. Essa funcionalidade tem o objetivo de impedir que agentes mal-intencionados acessem a rede interna da organização pela Internet ou usem serviços, protocolos ou portas de maneira não autorizada. Quando essa funcionalidade é fornecida como um recurso integrado de um NSC, a entidade deve garantir que suas configurações não resultem na desativação ou desvio da funcionalidade. **Definições** Manter o "estado" (ou status) para cada conexão em uma rede significa que o NSC "sabe" se uma resposta aparente a uma conexão anterior é uma resposta válida e autorizada (uma vez que o NSC retém o status de cada conexão) ou se é um tráfego malicioso tentando enganar o NSC para permitir a conexão.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **1.4.3** Medidas antifalsificação são implementadas para detectar e impedir que endereços IP de origem forjados entrem na rede confiável. **Objetivo da Abordagem Personalizada** Os pacotes com endereços de origem IP forjados não podem entrar em uma rede confiável.	**Procedimentos de Teste da Abordagem Definida** **1.4.3** Examine a documentação e as configurações do fornecedor para os NSCs para verificar se as medidas antifalsificação são implementadas para detectar e impedir que endereços IP de origem forjados entrem na rede confiável.	**Objetivo** A filtragem de pacotes que entram na rede confiável ajuda, entre outras coisas, a garantir que os pacotes não sejam "falsificados" para parecerem vindos da própria rede interna de uma organização. Por exemplo, medidas antifalsificação evitam que endereços internos originados da Internet passem para a DMZ. **Práticas Recomendadas** Os produtos geralmente vêm com o antifalsificação definido como padrão e podem não ser configuráveis. As entidades devem consultar a documentação do fornecedor para obter mais informações. **Exemplos** Normalmente, um pacote contém o endereço IP do computador que o enviou originalmente para que outros computadores na rede saibam de onde o pacote se originou. Indivíduos mal-intencionados frequentemente tentarão falsificar (ou imitar) o endereço IP de envio para enganar o sistema de destino e fazê-lo acreditar que o pacote é de uma fonte confiável.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
1.4.4 Os componentes do sistema que armazenam dados do titular do cartão não podem ser acessados diretamente de redes não confiáveis.	**1.4.4.a** Examine o diagrama de fluxo de dados e o diagrama de rede para verificar se está documentado que os componentes de sistema que armazenam os dados do titular do cartão não podem ser acessados diretamente nas redes não confiáveis.	Os dados do titular do cartão que podem ser acessados diretamente de uma rede não confiável, por exemplo, porque estão armazenados em um sistema dentro da DMZ ou em um serviço de banco de dados em nuvem, são mais fáceis de acessar por um invasor externo porque há menos camadas de defesa para penetrar. O uso dos NSCs para garantir que os componentes do sistema que armazenam os dados do titular do cartão (como um banco de dados ou um arquivo) só possam ser acessados diretamente de redes confiáveis pode evitar que o tráfego de rede não autorizado alcance o componente do sistema.
Objetivo da Abordagem Personalizada	**1.4.4.b** Examine as configurações dos NSCs para verificar se os controles são implementados de forma que os componentes de sistema que armazenam os dados do titular do cartão não possam ser acessados diretamente em redes não confiáveis.	
Os dados armazenados do titular do cartão não podem ser acessados de redes não confiáveis.		
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).		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Restringir a divulgação de endereços IP internos, privados e locais é útil para evitar que um hacker obtenha conhecimento desses endereços IP e use essas informações para acessar a rede. **Práticas Recomendadas** Os métodos usados para atender ao objetivo deste requisito podem variar, dependendo da tecnologia de rede específica que está sendo usada. Por exemplo, os controles utilizados para satisfazer esse requisito podem ser diferentes para as redes IPv4 em comparação com as redes IPv6. **Exemplos** Métodos para obscurecer o endereçamento IP podem incluir, mas não estão limitados a: • IPv4 Network Address Translation (NAT). • Colocar componentes de sistema atrás de servidores proxy/NSCs. • Remoção ou filtragem de anúncios de rota para redes internas que usam endereçamento registrado. • Uso interno da RFC 1918 (IPv4) ou usar extensão de privacidade do IPv6 (RFC 4941) ao iniciar sessões de saída para a Internet.
1.4.5 A divulgação de endereços IP internos e informações de roteamento é limitada apenas a partes autorizadas.	**1.4.5.a** Examine as configurações dos NSCs para verificar se a divulgação de endereços IP internos e informações de roteamento é limitada apenas a partes autorizadas.	
	1.4.5.b Entreviste a equipe e examine a documentação para verificar se os controles são implementados de forma que qualquer divulgação de endereços IP internos e informações de roteamento seja limitada apenas a partes autorizadas.	
Objetivo da Abordagem Personalizada		
As informações da rede interna são protegidas contra divulgação não autorizada.		

Requisitos e Procedimentos de Teste		Diretriz
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.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Os dispositivos de computação que têm permissão para se conectar à Internet de fora do ambiente corporativo - por exemplo, desktops, laptops, tablets, smartphones e outros dispositivos de computação móveis usados pelos funcionários - são mais vulneráveis a ameaças baseadas na Internet. Uso de controles de segurança, como controles baseados em host (por exemplo, software de firewall pessoal ou soluções de proteção de endpoint), controles de segurança baseados em rede (por exemplo, firewalls, inspeção baseada em heurística de rede e simulação de malware) ou hardware, ajuda a proteger os dispositivos de ataques baseados na Internet, que podem usar o dispositivo para obter acesso aos sistemas e dados da organização quando o dispositivo for reconectado à rede. **Práticas Recomendadas** As definições de configuração específicas são determinadas pela entidade e devem ser consistentes com suas políticas e procedimentos de segurança de rede. Onde houver uma necessidade legítima de desativar temporariamente os controles de segurança em um dispositivo de propriedade da empresa ou do funcionário que se conecta a uma rede não confiável e ao CDE - por exemplo, para dar suporte a uma atividade de manutenção específica ou investigação de um problema técnico - o motivo para tomar tal ação é entendido e aprovado por um representante da administração apropriado. *(continua na página a seguir)*
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 alterados pelos usuários dos dispositivos de computação, a menos que especificamente documentados e autorizados pela administração, caso a caso, por um período limitado.	**1.5.1.a** Examine as políticas e os padrões de configuração e entreviste a equipe para verificar se os controles de segurança dos dispositivos de computação que se conectam a redes não confiáveis e ao CDE são implementados de acordo com todos os elementos especificados neste requisito. **1.5.1.b** Examine as definições de configuração nos dispositivos de computação que se conectam a redes não confiáveis e ao CDE para verificar se as configurações estão implementadas de acordo com todos os elementos especificados neste requisito.	

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Dispositivos que se conectam a ambientes não confiáveis e também se conectam ao CDE não podem introduzir ameaças ao CDE da entidade.		Qualquer desativação ou alteração desses controles de segurança, incluindo nos próprios dispositivos dos administradores, é realizada por pessoal utorizado. É reconhecido que os administradores têm privilégios que podem permitir que desabilitem os controles de segurança em seus próprios computadores, mas devem haver mecanismos de alerta quando esses controles são desabilitados e o acompanhamento que ocorre para garantir que os processos sejam seguidos. **Exemplos** As práticas incluem a proibição do túnel dividido de VPNs para dispositivos móveis de propriedade de funcionários ou corporativos e exigir que tais dispositivos sejam inicializados em uma VPN.
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, eles deverão ser formalmente autorizados. Também podem ser necessárias medidas de segurança adicionais para o período durante o qual esses controles de segurança não estão ativos. Este requisito se aplica a dispositivos de computação de propriedade de funcionários e da empresa. 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 de Sistema

Seções
2.1 Processos e mecanismos para aplicar configurações seguras em todos os componentes de sistema são definidos e compreendidos.
2.2 Os componentes de sistema são configurados e administrados com segurança.
2.3 Os ambientes wireless são configurados e administrados com segurança.

Visão Geral

Indivíduos mal-intencionados, tanto externos quanto internos a uma entidade, costumam usar senhas padrão e configurações padrão de outros fornecedores para comprometer os sistemas. Essas senhas e configurações são bem conhecidas e facilmente determinadas por meio de informações públicas.

Aplicar configurações seguras aos componentes de sistema reduz os meios disponíveis para um invasor comprometer o sistema. A alteração de senhas padrão, a remoção de software, funções e contas desnecessárias e a desativação ou remoção de serviços desnecessários ajudam a reduzir a superfície de ataque potencial.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
2.1 Processos e mecanismos para aplicar configurações seguras em todos os componentes de sistema são definidos e compreendidos.		
Requisitos da Abordagem Definida **2.1.1** Todas as políticas e processos operacionais identificados no Requisito 2 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 2 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **2.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 2 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 2.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 2. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 2, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
2.1.2 As funções e responsabilidades para a execução de atividades no Requisito 2 são documentadas, atribuídas e compreendidas.	**2.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 2 estão documentadas e atribuídas.	
	2.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 2 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 2 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
2.2 Os componentes de sistema são configurados e administrados com segurança.		
Requisitos da Abordagem Definida **2.2.1** Os padrões de configuração são desenvolvidos, implementados e mantidos para: • Cobrir todos os componentes de sistema. • Abordar todas as vulnerabilidades de segurança conhecidas. • Ser consistente com os padrões de proteção de sistemas aceitos pela indústria 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 implementados antes ou imediatamente após um componente de sistema ser conectado a um ambiente de produção. **Objetivo da Abordagem Personalizada** Todos os componentes de sistema são configurados de forma segura e consistente e de acordo com os padrões de proteção aceitos pela indústria ou recomendações do fornecedor.	**Procedimentos de Teste da Abordagem Definida** **2.2.1.a** Examine os padrões de configuração do sistema para verificar se eles definem os processos que incluem todos os elementos especificados neste requisito. **2.2.1.b** Examine as políticas e procedimentos e entreviste a equipe para verificar se os padrões de configuração do sistema são atualizados à medida que novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.3.1. **2.2.1.c** Examine as definições de configuração e entreviste a equipe para verificar se os padrões de configuração de sistemas são aplicados quando novos sistemas são configurados e verificados como estando implementados antes ou imediatamente após um componente de sistema ser conectado a um ambiente de produção.	**Objetivo** Existem pontos fracos conhecidos com muitos sistemas operacionais, bancos de dados, dispositivos de rede, software, aplicativos, imagens de contêiner e outros dispositivos usados por uma entidade ou dentro do ambiente de uma entidade. Também existem maneiras conhecidas de configurar esses componentes de sistema para corrigir vulnerabilidades de segurança. A correção de vulnerabilidades de segurança reduz as oportunidades disponíveis para um invasor. Ao desenvolver padrões, as entidades garantem que seus componentes de sistema sejam configurados de forma consistente e segura e lidam com a proteção de dispositivos para os quais a proteção total pode ser mais difícil. **Práticas Recomendadas** Manter-se atualizado com as orientações atuais da indústria ajudará a entidade a manter configurações seguras. Os controles específicos a serem aplicados a um sistema variam e devem ser apropriados para o tipo e função do sistema. Várias organizações de segurança estabeleceram diretrizes e recomendações de fortalecimento de sistema, que aconselham como corrigir pontos fracos conhecidos e comuns. **Informações Adicionais** As fontes de orientação sobre os padrões de configuração incluem, mas não estão limitadas a: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance e fornecedores de produtos.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**2.2.2.a** Examine os padrões de configuração do sistema para verificar se eles incluem o gerenciamento de contas padrão do fornecedor de acordo com todos os elementos especificados neste requisito. **2.2.2.b** Examine a documentação do fornecedor e observe um administrador do sistema fazendo logon usando contas padrão do fornecedor para verificar se as contas estão implementadas de acordo com todos os elementos especificados neste requisito. **2.2.2.c** Examine os arquivos de configuração e entreviste a equipe para verificar se todas as contas padrão do fornecedor que não serão usadas foram removidas ou desabilitadas.	Indivíduos mal-intencionados geralmente usam nomes de contas e senhas padrão do fornecedor para comprometer os sistemas operacionais, aplicativos e os sistemas nos quais estão instalados. Como essas configurações padrão são frequentemente publicadas e bem conhecidas, a alteração dessas configurações tornará os sistemas menos vulneráveis a ataques. **Práticas Recomendadas** Todas as contas padrão do fornecedor devem ser identificadas e sua finalidade e uso entendidos. É importante estabelecer controles para contas de aplicativo e sistema, incluindo aqueles usados para implantar e manter serviços em nuvem para que não usem senhas padrão e não sejam utilizáveis por pessoas não autorizadas. Quando uma conta padrão não se destina a ser usada, alterar a senha padrão para uma senha única que atenda ao Requisito 8.3.6 do PCI DSS, remover qualquer acesso à conta padrão e, em seguida, desativar a conta, impedirá que um indivíduo mal-intencionado volte a habilitar a conta e obtenha acesso com a senha padrão. O uso de uma rede de teste isolada para instalar e configurar novos sistemas é recomendado e também pode ser usado para confirmar se as credenciais padrão não foram introduzidas em ambientes de produção. **Exemplos** Os padrões a serem considerados incluem IDs de usuário, senhas e outras credenciais de autenticação geralmente usadas por fornecedores em seus produtos.
Objetivo da Abordagem Personalizada		
Os componentes de sistema não podem ser acessados com senhas padrão.		
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 do Protocolo de Gerenciamento de Rede Simples (SNMP, por seu acrônimo em inglês). Este requisito também se aplica quando um componente de 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 de sistema, **OU** • As funções primárias com diferentes níveis de segurança que existem no mesmo componente de sistema são isoladas umas das outras, **OU** • As funções primárias com diferentes níveis de segurança no mesmo componente de sistema são todas protegidas no nível exigido pela função com a mais alta necessidade de segurança.	**2.2.3.a** Examine os padrões de configuração do sistema para verificar se eles incluem o gerenciamento de funções primárias que requerem diferentes níveis de segurança, tal como especificado neste requisito. **2.2.3.b** Examine as configurações dos sistemas para verificar se as funções primárias que requerem diferentes níveis de segurança são gerenciadas por uma das formas especificadas neste requisito. **2.2.3.c** Onde as tecnologias de virtualização são usadas, examine as configurações do sistema para verificar se as funções do sistema que requerem diferentes níveis de segurança são gerenciadas de uma das seguintes maneiras: • Funções com necessidades de segurança diferentes não coexistem no mesmo componente de sistema. • Funções com necessidades de segurança diferentes que existem no mesmo componente de sistema são isoladas umas das outras. • Funções com diferentes necessidades de segurança no mesmo componente de sistema são todas protegidas no nível exigido pela função com a mais alta necessidade de segurança.	Os sistemas que contêm uma combinação de serviços, protocolos e daemons para sua função primária terão um perfil de segurança apropriado para permitir que essa função opere com eficácia. Por exemplo, os sistemas que precisam estar diretamente conectados à Internet têm um perfil específico, como um servidor DNS, servidor web ou servidor de comércio eletrônico. Por outro lado, outros componentes de sistema podem operar uma função primária compreendendo um conjunto diferente de serviços, protocolos e daemons que executam funções que uma entidade não deseja expor na Internet. Este requisito visa garantir que funções diferentes não afetem os perfis de segurança de outros serviços de uma forma que possa fazer com que operem em um nível de segurança superior ou inferior. **Práticas Recomendadas** Em um cenário ideal, cada função deve ser colocada em diferentes componentes de sistema. Isso pode ser alcançado implementando apenas uma função primária em cada componente de sistema. Outra opção é isolar funções primárias no mesmo componente de sistema que têm níveis de segurança diferentes, por exemplo, isolar servidores web (que precisam ser conectados diretamente à Internet) de servidores de aplicativos e de banco de dados. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
As funções primárias com necessidades de segurança mais baixas não podem afetar a segurança das funções primárias com necessidades de segurança mais altas no mesmo componente de sistema.		

Requisitos e Procedimentos de Teste		Diretriz
		Se um componente de sistema contém funções primárias que precisam de diferentes níveis de segurança, uma terceira opção é implementar controles adicionais para garantir que o nível de segurança resultante da(s) função(ões) primária(s) com necessidades de segurança mais altas não seja reduzido pela presença de funções primárias de segurança inferior. Além disso, as funções com um nível de segurança mais baixo devem ser isoladas e/ou protegidas para garantir que não possam acessar ou afetar os recursos de outra função do sistema e não introduzam fragilidades de segurança para outras funções no mesmo servidor. Funções de diferentes níveis de segurança podem ser isoladas por controles físicos ou lógicos. Por exemplo, um sistema de banco de dados também não deve hospedar serviços web, a menos que use controles como tecnologias de virtualização para isolar e conter as funções em subsistemas separados. Outro exemplo é usar instâncias virtuais ou fornecer acesso dedicado à memória por função do sistema. Onde as tecnologias de virtualização são usadas, os níveis de segurança devem ser identificados e gerenciados para cada componente virtual. Exemplos de considerações para ambientes virtualizados incluem: • A função de cada aplicativo, contêiner ou instância de servidor virtual. • Como as máquinas virtuais (VMs) ou contêineres são armazenados e protegidos.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
2.2.4 Apenas os serviços, protocolos, daemons e funções necessários são ativados e todas as funcionalidades desnecessárias são removidas ou desativadas.	**2.2.4.a** Examine os padrões de configuração do sistema para verificar se os serviços, protocolos e daemons do sistema necessários são identificados e documentados.	Serviços e funções desnecessários podem fornecer oportunidades adicionais para indivíduos mal-intencionados obterem acesso a um sistema. Ao remover ou desabilitar todos os serviços, protocolos, daemons e funções desnecessários, as organizações podem se concentrar em proteger as funções necessárias e reduzir o risco de que funções desconhecidas ou desnecessárias sejam exploradas.
Objetivo da Abordagem Personalizada	**2.2.4.b** Examine as configurações de sistema para verificar o seguinte: • Toda as funcionalidades desnecessárias são removidas ou desabilitadas. • Apenas a funcionalidade necessária é habilitada, conforme documentado nos padrões de configuração.	**Práticas Recomendadas** Existem muitos protocolos que podem ser ativados por padrão e são comumente usados por indivíduos mal-intencionados para comprometer uma rede. Desativar ou remover todos os serviços, funções e protocolos que não são usados minimiza a superfície de ataque potencial - por exemplo, removendo ou desativando um FTP ou servidor web não usado. **Exemplos** Funcionalidades desnecessárias podem incluir, mas não se limitam a scripts, drivers, recursos, subsistemas, sistemas de arquivos, interfaces (USB e Bluetooth) e servidores web desnecessários.
Os componentes de sistema não podem ser comprometidos pela exploração de funcionalidades desnecessárias presentes no componente de sistema.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Garantir que todos os serviços, protocolos e daemons não seguros sejam adequadamente protegidos com recursos de segurança apropriados torna mais difícil que indivíduos mal-intencionados explorem pontos comuns de comprometimento em uma rede. **Práticas Recomendadas** Habilitar recursos de segurança antes que novos componentes de sistema sejam implantados impedirá que configurações inseguras sejam introduzidas no ambiente. Algumas soluções de fornecedores podem fornecer funções de segurança adicionais para ajudar a proteger um processo inseguro. **Informações Adicionais** Para obter orientação sobre serviços, protocolos ou daemons considerados inseguros, consulte os padrões e orientações da indústria (por exemplo, tal como publicado pelo NIST, ENISA e OWASP).
2.2.5 Se algum serviço, protocolo ou daemons não seguro estiver presente: • A justificativa comercial é documentada. • Recursos de segurança adicionais são documentados e implementados para reduzir o risco de usar serviços, protocolos ou daemons inseguros.	**2.2.5.a** Se quaisquer serviços, protocolos ou daemons inseguros estiverem presentes, examine os padrões de configuração do sistema e entreviste o pessoal para verificar se são gerenciados e implementados de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada	**2.2.5.b** Se quaisquer serviços, protocolos ou daemons inseguros estiverem presentes, examine as definições de configuração para verificar se os recursos de segurança adicionais foram implementados para reduzir o risco de usar serviços, daemons e protocolos inseguros.	
Os componentes de sistema não podem ser comprometidos pela exploração de serviços, protocolos ou daemons inseguros.		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
A configuração correta dos parâmetros de segurança fornecidos nos componentes de sistema aproveita os recursos do componente de sistema para derrotar ataques maliciosos.
Práticas Recomendadas
Os padrões de configuração dos sistemas e processos relacionados devem abordar especificamente as configurações e parâmetros de segurança que têm implicações de segurança conhecidas para cada tipo de sistema em uso.
Para que os sistemas sejam configurados com segurança, o pessoal responsável pela configuração e/ou administração dos sistemas deve ter conhecimento dos parâmetros e configurações de segurança específicos que se aplicam aos sistemas. As considerações também devem incluir configurações seguras para parâmetros usados para acessar portais em nuvem.
Informações Adicionais
Consulte a documentação do fornecedor e as referências da indústria observadas no Requisito 2.2.1 para obter informações sobre os parâmetros de segurança aplicáveis para cada tipo de sistema.</td></tr>
<tr><td rowspan="3">2.2.6 Os parâmetros de segurança dos sistemas são configurados para evitar o uso indevido.</td><td>2.2.6.a Examine os padrões de configuração do sistema para verificar se incluem a configuração dos parâmetros de segurança do sistema para evitar o uso indevido.</td></tr>
<tr><td>2.2.6.b Entreviste os administradores dos sistemas e/ou gerentes de segurança para verificar se têm conhecimento das configurações de parâmetros de segurança comuns para os componentes de sistema.</td></tr>
<tr><td rowspan="2">2.2.6.c Examine as configurações de sistema para verificar se os parâmetros de segurança comuns estão definidos apropriadamente e de acordo com os padrões de configuração dos sistemas.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada</td></tr>
<tr><td>Os componentes de sistema não podem ser comprometidos devido à configuração incorreta dos parâmetros de segurança.</td><td></td><td></td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
2.2.7 Todo o acesso administrativo não-console é criptografado usando criptografia forte.	**2.2.7.a** Examine os padrões de configuração do sistema para verificar se eles incluem criptografar todos os acessos administrativos não-console usando criptografia forte.	**Objetivo** Se a administração não-console (incluindo remota) não usar comunicações criptografadas, fatores de autorização administrativa (como IDs e senhas) podem ser revelados a um intruso. Um indivíduo mal-intencionado pode usar essas informações para acessar a rede, tornar-se administrador e roubar dados. **Práticas Recomendadas** Qualquer que seja o protocolo de segurança usado, ele deve ser configurado para usar apenas versões e configurações seguras a fim de evitar o uso de uma conexão insegura - por exemplo, usando apenas certificados confiáveis, suportando apenas criptografia forte e não suportando falhas para protocolos ou métodos mais fracos e inseguros . **Exemplos** Os protocolos de texto não criptografado (como HTTP, telnet, etc.) não criptografam detalhes de tráfego ou logon, tornando mais fácil para um intruso interceptar essas informações. O acesso não-console pode ser facilitado por tecnologias que fornecem acesso alternativo aos sistemas, incluindo, mas não se limitando a, out-of-band (OOB), lights-out management (LOM), Intelligent Platform Management Interface (IPMI) e switches de teclado, vídeo e mouse (KVM) com recursos remotos. Essas e outras tecnologias e métodos de acesso não-console devem ser protegidos com criptografia forte. **Informações Adicionais** Consulte os padrões da indústria e as práticas recomendadas, como *NIST SP 800-52 e SP 800-57.*
	2.2.7.b Observe um administrador efetuar logon nos componentes de sistema e examine as configurações dos sistemas para verificar se o acesso administrativo não-console é gerenciado de acordo com este requisito.	
	2.2.7.c Examine as configurações dos componentes de sistema e dos serviços de autenticação para verificar se os serviços de login remoto inseguros não estão disponíveis para acesso administrativo não-console.	
	2.2.7.d Examine a documentação do fornecedor e entreviste a equipe para verificar se a criptografia forte para a tecnologia em uso está implementada de acordo com as práticas recomendadas da indústria e/ou recomendações do fornecedor.	
Objetivo da Abordagem Personalizada		
Os fatores de autorização administrativa de texto não criptografado não podem ser lidos ou interceptados em nenhuma transmissão de rede.		
Observações de Aplicabilidade		
Isso inclui acesso administrativo por meio de interfaces baseadas em navegador e interfaces de programação de aplicativos (APIs).		

Requisitos e Procedimentos de Teste		Diretriz
2.3 Os ambientes wireless são configurados e administrados com segurança.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
2.3.1 Para ambientes wireless conectados ao CDE ou transmitindo dados da conta, todos os padrões do fornecedor wireless são alterados na instalação ou são confirmados como seguros, incluindo, mas não se limitando a: • Chaves de criptografia wireless padrão. • Senhas em pontos de acesso wireless. • Padrões SNMP. • Quaisquer outros padrões de fornecedores wireless relacionados à segurança.	**2.3.1.a** Examine as políticas e procedimentos e entreviste o pessoal responsável para verificar se os processos estão definidos para os padrões do fornecedor wireless para alterá-los na instalação ou para confirmar que são seguros de acordo com todos os elementos deste requisito.	Se as redes wireless não forem implementadas com configurações de segurança suficientes (incluindo a alteração das configurações padrão), os sniffers wireless podem espionar o tráfego, capturar facilmente dados e senhas e entrar e atacar facilmente a rede. **Práticas Recomendadas** As senhas wireless devem ser construídas de forma que sejam resistentes a ataques de força bruta off-line.
	2.3.1.b Examine a documentação do fornecedor e observe o login do administrador do sistema em dispositivos wireless para verificar: • Os padrões SNMP não são usados. • As senhas/frases secretas padrão nos pontos de acesso wireless não são usadas.	
Objetivo da Abordagem Personalizada As redes wireless não podem ser acessadas usando senhas padrão do fornecedor ou configurações padrão.	**2.3.1.c** Examine a documentação do fornecedor e as definições de configuração wireless para verificar se outros padrões do fornecedor wireless relacionados à segurança foram alterados, se aplicável.	
Observações de Aplicabilidade Isso inclui, mas não está limitado a, chaves de criptografia wireless padrão, senhas em pontos de acesso wireless, padrões SNMP e quaisquer outros padrões de fornecedores wireless relacionados à segurança.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Alterar as chaves de criptografia wireless sempre que alguém com conhecimento da chave deixa a organização ou muda para uma função que não exija mais o conhecimento da chave ajuda a manter o conhecimento das chaves limitado apenas àqueles com necessidade comercial de conhecê-las. Além disso, alterar as chaves de criptografia wireless sempre que houver suspeita ou comprovação de que uma chave está comprometida torna a rede wireless mais resistente ao comprometimento. **Práticas Recomendadas** Esse objetivo pode ser alcançado de várias maneiras, incluindo mudanças periódicas de chaves, alterando chaves por meio de um processo definido como “joiners-movers-leavers” (JML), implementando controles técnicos adicionais e não usando chaves pré-compartilhadas fixas. Além disso, todas as chaves que são conhecidas ou suspeitas de estarem comprometidas devem ser gerenciadas de acordo com o plano de resposta a incidentes da entidade no Requisito 12.10.1.
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.	**2.3.2** Entreviste a equipe responsável e examine a documentação de gerenciamento de chaves para verificar se as chaves de criptografia wireless foram alteradas de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
O conhecimento das chaves de criptografia wireless não permite o acesso não autorizado a redes wireless.		

Proteger os Dados da Conta

Requisito 3: Proteja os Dados da Conta Armazenados

Seções	
3.1	Os processos e mecanismos para proteger os dados da conta armazenados são definidos e compreendidos.
3.2	O armazenamento de dados da conta é mínimo.
3.3	Os dados de autenticação confidenciais (SAD) não são armazenados após a autorização.
3.4	O acesso a exibição de PAN completo e a capacidade de copiar os dados do titular do cartão são restritos.
3.5	O número da conta principal (PAN) é protegido onde quer que seja armazenado.
3.6	As chaves criptográficas usadas para proteger os dados da conta armazenados são protegidas.
3.7	Onde a criptografia é usada para proteger os dados da conta armazenados, os processos e procedimentos de gerenciamento de chave cobrindo todos os aspectos do ciclo de vida da chave são definidos e implementados.

Visão Geral

Métodos de proteção como criptografia, truncamento, mascaramento e hashing são componentes essenciais da proteção de dados da conta. Se um invasor contornar outros controles de segurança e obtiver acesso aos dados da conta criptografados, os dados ficarão ilegíveis sem as chaves criptográficas adequadas e não poderão ser utilizados pelo invasor. Outros métodos eficazes de proteção de dados armazenados também devem ser considerados como oportunidades potenciais de mitigação de risco. Por exemplo, os métodos para minimizar o risco incluem não armazenar dados da conta, a menos que seja necessário, truncar os dados do titular do cartão se o PAN completo não for necessário e não enviar PANs desprotegidos usando tecnologias de mensagens de usuário final, como e-mail e mensagens instantâneas.

Se os dados da conta estiverem presentes na memória não persistente (por exemplo, RAM, memória volátil), a criptografia dos dados da conta não é necessária. No entanto, os controles adequados devem estar implementados para garantir que a memória mantenha um estado não persistente. Os dados devem ser removidos da memória volátil assim que o objetivo do negócio (por exemplo, a transação associada) for concluído. No caso do armazenamento de dados se tornar persistente, todos os Requisitos do PCI DSS aplicáveis serão considerados, incluindo a criptografia dos dados armazenados.

O Requisito 3 se aplica à proteção dos dados da conta armazenados, a menos que seja especificamente solicitado em um requisito individual.

Consulte o Apêndice G para obter as definições de “Criptografia Forte” e outros termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
3.1 Os processos e mecanismos para proteger os dados da conta armazenados são definidos e compreendidos.		
Requisitos da Abordagem Definida **3.1.1** Todas as políticas e processos operacionais identificados no Requisito 3 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 3 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **3.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 3 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 3.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 3. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 3, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
3.1.2 As funções e responsabilidades para a execução de atividades no Requisito 3 são documentadas, atribuídas e compreendidas.	**3.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 3 estão documentadas e atribuídas.	
	3.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 3 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 3 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
3.2 O armazenamento de dados da conta é mínimo.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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 da 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 observações de aplicabilidade abaixo para obter detalhes.* • Limitar a quantidade de armazenamento de dados e o tempo de retenção ao que é necessário para requisitos legais ou regulamentares e/ou de negócios. • Requisitos de retenção específicos para dados das 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.	**3.2.1.a** Examine as políticas, procedimentos e processos de retenção e descarte de dados e entreviste o pessoal para verificar se os processos estão definidos para incluir todos os elementos especificados neste requisito. **3.2.1.b** Examine os arquivos e registros do sistema nos componentes de sistema onde os dados da conta são armazenados para verificar se a quantidade de armazenamento de dados e o tempo de retenção não excedem os requisitos definidos na política de retenção de dados. **3.2.1.c** Observe os mecanismos usados para tornar os dados da conta irrecuperáveis para verificar se os dados não podem ser recuperados.	**Objetivo** Uma política de retenção de dados formal identifica quais dados precisam ser retidos, por quanto tempo e onde esses dados residem para que possam ser destruídos ou excluídos com segurança assim que não forem mais necessários. Os únicos dados da conta que podem ser armazenados após a autorização são o número da conta principal ou PAN (tornado ilegível), data de validade, nome do titular do cartão e código de serviço. O armazenamento de SAD antes da conclusão do processo de autorização também está incluído na política de retenção e descarte de dados, de modo que o armazenamento desses dados confidenciais seja mínimo e retido apenas pelo período de tempo definido. **Práticas Recomendadas** Ao identificar os locais dos dados da conta armazenados, considere todos os processos e pessoal com acesso aos dados, pois os dados podem ter sido movidos e armazenados em locais diferentes dos originalmente definidos. Os locais de armazenamento que costumam ser esquecidos incluem sistemas de backup e arquivamento, dispositivos removíveis de armazenamento de dados, mídia em papel e gravações de áudio. Para definir os requisitos de retenção apropriados, uma entidade primeiro precisa entender suas próprias necessidades de negócios, bem como quaisquer obrigações legais ou regulamentares que se aplicam a sua indústria ou ao tipo de dados que estão sendo retidos. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Os dados da conta são retidos apenas quando necessário e pelo menor tempo necessário e são excluídos com segurança ou tornados irrecuperáveis quando não são mais necessários. **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.*		Implementar um processo automatizado para garantir que os dados sejam excluídos de forma automática e segura após seu limite de retenção definido pode ajudar a garantir que os dados da conta não sejam retidos além do necessário para fins comerciais, legais ou regulatórios. Os métodos de eliminação de dados quando excedem o período de retenção incluem exclusão segura para a remoção completa dos dados ou torná-los irrecuperáveis e impossíveis de serem reconstruídos. Identificar e eliminar com segurança os dados armazenados que excederam o período de retenção especificado evita a retenção desnecessária de dados que não são mais necessários. Esse processo pode ser automatizado, manual ou uma combinação de ambos. A função de exclusão na maioria dos sistemas operacionais não é "exclusão segura", pois permite que os dados excluídos sejam recuperados; em vez disso, uma função ou aplicativo dedicado de exclusão segura deve ser usado para tornar os dados irrecuperáveis. *Lembre-se, se você não precisar, não armazene!* **Exemplos** Um procedimento automatizado e programático pode ser executado para localizar e remover dados, ou uma revisão manual das áreas de armazenamento de dados pode ser realizada. Qualquer que seja o método usado, é uma boa ideia monitorar o processo para garantir que ele seja concluído com êxito e que os resultados sejam registrados e validados como completos. A implementação de métodos de exclusão segura garante que os dados não possam ser recuperados quando não forem mais necessários. **Informações Adicionais** *Consulte o NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.*

Requisitos e Procedimentos de Teste		Diretriz
3.3 Os dados de autenticação confidenciais (SAD) não são armazenados após a autorização.		
Requisitos da Abordagem Definida **3.3.1** O SAD não é retido após a autorização, mesmo se criptografado. Todos os dados de autenticação confidenciais recebidos são tornados irrecuperáveis após a conclusão do processo de autorização. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **Observações de Aplicabilidade** Este requisito não se aplica a emissores e empresas que oferecem suporte a serviços de emissão (onde o SAD é necessário para uma necessidade comercial de emissão legítima) e têm uma justificativa comercial para armazenar os dados de autenticação confidenciais. Consulte o Requisito 3.3.3 para requisitos adicionais específicos para emissores. Os dados de autenticação confidenciais incluem os dados citados nos Requisitos 3.3.1.1 a 3.3.1.3.	**Procedimentos de Teste da Abordagem Definida** **3.3.1.a** Se o SAD for recebido, examine as políticas, procedimentos e configurações dos sistemas documentados para verificar se os dados não são retidos após a autorização. **3.3.1.b** Se o SAD for recebido, examine os procedimentos documentados e observe os processos de exclusão de dados seguros para verificar se os dados são tornados irrecuperáveis após a conclusão do processo de autorização.	**Objetivo** O SAD é muito valioso para indivíduos mal-intencionados, pois permite que eles gerem cartões de pagamento falsificados e criem transações fraudulentas. Portanto, o armazenamento do SAD após a conclusão do processo de autorização é proibido. **Definições** O processo de autorização é concluído quando um comerciante recebe uma resposta da transação (por exemplo, uma aprovação ou recusa).

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **3.3.1.1** O conteúdo completo de qualquer trilha não é retido após a conclusão do processo de autorização. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **Observações de Aplicabilidade** No curso normal dos negócios, os seguintes elementos de dados da trilha podem precisar ser retidos: • Nome do Titular do Cartão. • Número da Conta Principal (PAN). • Data de Validade. • Código de Serviço. Para minimizar o risco, armazene com segurança apenas esses elementos de dados conforme necessário para os negócios.	**Procedimentos de Teste da Abordagem Definida** **3.3.1.1** Examine as fontes de dados para verificar se o conteúdo completo de qualquer trilha não é armazenado após a conclusão do processo de autorização.	**Objetivo** Se o conteúdo completo de qualquer trilha (da tarja magnética no verso de um cartão, se houver, dados equivalentes contidos em um chip ou em outro lugar) for armazenado, indivíduos mal-intencionados que obtiverem esses dados podem usá-los para reproduzir cartões de pagamento e concluir transações fraudulentas . **Definições** Os dados de trilha completo são alternativamente chamados de trilha completa, trilha, trilha 1, trilha 2 e dados de tarja magnética. Cada trilha contém vários elementos de dados e este requisito especifica apenas aqueles que podem ser retidos após a autorização. **Exemplos** Fontes de dados a serem revisadas para garantir que o conteúdo completo de qualquer trilha não seja retido após a conclusão do processo de autorização incluem, mas não estão limitados a: • Dados de transação de entrada. • Todos os registros (por exemplo, transação, histórico, depuração, erro) • Arquivos de histórico. • Arquivos de rastreamento. • Esquemas de banco de dados. • Conteúdo de bancos de dados e armazenamentos de dados locais e na nuvem. • Quaisquer arquivos de despejo de memória/travamento existentes.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **3.3.1.2** O código de verificação do cartão não é retido após a conclusão do processo de autorização. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **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.	**Procedimentos de Teste da Abordagem Definida** **3.3.1.2** Examine as fontes de dados para verificar se o código de verificação do cartão não está armazenado após a conclusão do processo de autorização.	**Objetivo** Se os dados do código de verificação do cartão forem roubados, indivíduos mal-intencionados podem executar transações fraudulentas pela Internet e por telefone/correio (MO/TO). Não armazenar esses dados reduz a probabilidade de eles serem comprometidos. **Exemplos** Se os códigos de verificação do cartão forem armazenados em mídia de papel antes da conclusão da autorização, um método para apagar ou cobrir os códigos deve impedir que eles sejam lidos após a autorização ser concluída. Exemplos de métodos para tornar os códigos ilegíveis incluem remover o código com uma tesoura e aplicar um marcador opaco e não removível adequado sobre o código. As fontes de dados a serem revisadas para garantir que o código de verificação do cartão não seja retido após a conclusão do processo de autorização incluem, mas não estão limitadas a: • Dados de transação de entrada. • Todos os registros (por exemplo, transação, histórico, depuração, erro) • Arquivos de histórico. • Arquivos de rastreamento. • Esquemas de banco de dados. • Conteúdo de bancos de dados e armazenamentos de dados locais e na nuvem. • Quaisquer arquivos de despejo de memória/travamento existentes.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **3.3.1.3** O número de identificação pessoal (PIN) e o bloco de PIN não são retidos após a conclusão do processo de autorização. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **Observações de Aplicabilidade** Os blocos de PIN são criptografados durante o curso natural dos processos de transação, mas mesmo se uma entidade criptografar o bloco de PIN novamente, ele ainda não poderá ser armazenado após a conclusão do processo de autorização.	**Procedimentos de Teste da Abordagem Definida** **3.3.1.3** Examine as fontes de dados para verificar se os PINs e blocos de PIN não são armazenados após a conclusão do processo de autorização.	**Objetivo** Os blocos de PIN e o PIN devem ser conhecidos apenas pelo proprietário do cartão ou pela entidade que emitiu o cartão. Se esses dados forem roubados, indivíduos mal-intencionados podem executar transações fraudulentas com base no PIN (por exemplo, compras na loja e saques em caixas eletrônicos). Não armazenar esses dados reduz a probabilidade de eles serem comprometidos. **Exemplos** As fontes de dados a serem revisadas para garantir que os blocos de PIN e o PIN não sejam retidos após a conclusão do processo de autorização incluem, mas não estão limitados a: • Dados de transação de entrada. • Todos os registros (por exemplo, transação, histórico, depuração, erro) • Arquivos de histórico. • Arquivos de rastreamento. • Esquemas de banco de dados. • Conteúdo de bancos de dados e armazenamentos de dados locais e na nuvem. • Quaisquer arquivos de despejo de memória/travamento existentes.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **3.3.2** O SAD que é armazenado eletronicamente antes da conclusão da autorização é criptografado usando criptografia forte. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **Observações de Aplicabilidade** Se o SAD tem permissão para ser armazenado antes da autorização é determinado pelas organizações que gerenciam programas de conformidade (por exemplo, bandeiras de pagamento e adquirentes). Contate as organizações de interesse 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. Este requisito não se aplica a emissores e empresas que oferecem suporte a serviços de emissão onde há uma justificativa comercial de emissão legítima para armazenar SAD. Consulte o Requisito 3.3.3 para requisitos específicos para emissores. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **3.3.2** Examine os armazenamentos de dados, configurações do sistema e/ou documentação do fornecedor para verificar se todo o SAD armazenado eletronicamente antes da conclusão da autorização é criptografado usando criptografia forte.	**Objetivo** O SAD pode ser usado por indivíduos mal-intencionados para aumentar a probabilidade de gerar cartões de pagamento falsificados e transações fraudulentas. **Práticas Recomendadas** As entidades devem considerar a criptografia do SAD com uma chave criptográfica diferente da usada para criptografar o PAN. Observe que isso não significa que o PAN presente no SAD (como parte dos dados de trilha) precisaria ser criptografado separadamente. **Definições** O processo de autorização é concluído assim que a resposta a uma resposta de solicitação de autorização, ou seja, uma aprovação ou recusa, é recebida.

Requisitos e Procedimentos de Teste		Diretriz
Este requisito não se aplica a emissores e empresas que oferecem suporte a serviços de emissão onde há uma justificativa comercial de emissão legítima para armazenar SAD. Consulte o Requisito 3.3.3 para requisitos específicos para emissores. Esse requisito não substitui como os blocos de PIN devem ser gerenciados, nem significa que um bloco 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
3.3.3 ***Requisito adicional para emissores e empresas que oferecem suporte a serviços de emissão e armazenam dados de autenticação confidenciais:*** Todo armazenamento de dados de autenticação confidenciais é: • Limitado ao que é necessário para uma necessidade comercial legítima de emissão e que está protegida. • Criptografado usando criptografia forte. *Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes.*	**3.3.3.a** ***Procedimento de teste adicional para emissores e empresas que oferecem suporte a serviços de emissão e armazenam dados de autenticação confidenciais:*** Examine as políticas documentadas e entreviste a equipe para verificar se há uma justificativa comercial documentada para o armazenamento de dados de autenticação confidenciais. **3.3.3.b** ***Procedimento de teste adicional para emissores e empresas que oferecem suporte a serviços de emissão e armazenam dados de autenticação confidenciais:*** Examine os armazenamentos de dados e as configurações dos sistemas para verificar se os dados de autenticação confidenciais estão armazenados com segurança.	O SAD pode ser usado por indivíduos mal-intencionados para aumentar a probabilidade de gerar cartões de pagamento falsificados e transações fraudulentas**.** **Práticas Recomendadas** As entidades devem considerar a criptografia do SAD com uma chave criptográfica diferente da usada para criptografar o PAN. Observe que isso não significa que o PAN presente no SAD (como parte dos dados de trilha) precisaria ser criptografado separadamente. **Definições** A necessidade legítima de negócios de emissão significa que os dados são necessários para facilitar o processo de negócios de emissão. **Informações Adicionais** *Consulte ISO/DIS 9564-5 Financial services — Personal Identification Number (PIN) management and security — Part 5: Methods for the generation, change, and verification of PINs and card security data using the advanced encryption standard.*
Objetivo da Abordagem Personalizada		
Os dados de autenticação confidenciais são retidos apenas conforme necessário para dar suporte às funções de emissão e são protegidos contra acesso não autorizado.		
Observações de Aplicabilidade		
Este requisito se aplica apenas a emissores e empresas que oferecem suporte a serviços de emissão e armazenam dados de autenticação confidenciais. As entidades que emitem cartões de pagamento ou que executam ou apoiam serviços de emissão geralmente criam e controlam dados de autenticação confidenciais como parte da função de emissão. É permitido às empresas que realizam, facilitam ou oferecem suporte a serviços de emissão armazenar dados de autenticação confidenciais SOMENTE SE tiverem uma necessidade comercial legítima de armazenar tais dados. *(continua na página a seguir)*		

Requisitos e Procedimentos de Teste		Diretriz
Os requisitos do PCI DSS destinam-se a todas as entidades que armazenam, processam ou transmitem dados da conta, incluindo emissores. A única exceção para emissores e processadores de emissores é que os dados de autenticação confidenciais podem ser retidos se houver um motivo legítimo para isso. Todos esses dados devem ser armazenados com segurança e de acordo com todos os requisitos do PCI DSS e requisitos das bandeiras de pagamento específicos. *O marcador acima (para criptografar o SAD armazenado com criptografia forte) é uma prática recomendada até 31 de março de 2025, após o qual será exigido como parte do Requisito 3.3.3 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*		

Requisitos e Procedimentos de Teste		Diretriz
3.4 O acesso a exibição de PAN completo e capacidade de copiar os dados do titular do cartão são restritos.		
Requisitos da Abordagem Definida **3.4.1** O PAN é mascarado quando exibido (o BIN 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 BIN e os quatro últimos dígitos do PAN. **Objetivo da Abordagem Personalizada** A exibição do PAN é restrita ao número mínimo de dígitos necessários para atender a uma necessidade comercial definida. **Observações de Aplicabilidade** Esse requisito não substitui os requisitos mais rígidos implementados para exibição de dados do titular do cartão - por exemplo, requisitos legais 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.	**Procedimentos de Teste da Abordagem Definida** **3.4.1.a** Examine as políticas e procedimentos documentados para mascarar a exibição de PANs para verificar: • Uma lista de funções que precisam de acesso a mais do que o BIN e os últimos quatro dígitos do PAN (inclui o PAN completo) é documentada, junto com a necessidade comercial legítima de cada função para ter esse acesso. • O PAN é mascarado quando exibido de forma que apenas o pessoal com uma necessidade comercial legítima possa ver mais do que o BIN e os últimos quatro dígitos do PAN. • Todas as funções não especificamente autorizadas para ver o PAN completo devem ver apenas PANs mascarados. **3.4.1.b** Examine as configurações dos sistemas para verificar se o PAN completo é exibido apenas para funções com uma necessidade comercial documentada e se o PAN está mascarado para todas as outras solicitações.	**Objetivo** A exibição do PAN completo em telas de computador, recibos de cartão de pagamento, relatórios em papel, etc. pode resultar na obtenção desses dados por pessoas não autorizadas e no uso fraudulento. Garantir que o PAN completo seja exibido apenas para aqueles com uma necessidade comercial legítima minimiza o risco de pessoas não autorizadas obterem acesso aos dados do PAN. **Práticas Recomendadas** Aplicar controles de acesso de acordo com as funções definidas é uma maneira de limitar o acesso à visualização do PAN completo apenas aos indivíduos com uma necessidade comercial definida. A abordagem de mascaramento deve sempre exibir apenas o número de dígitos necessários para executar uma função de negócios específica. Por exemplo, se apenas os quatro últimos dígitos forem necessários para executar uma função comercial, o PAN deve ser mascarado para mostrar apenas os quatro últimos dígitos. Como outro exemplo, se uma função precisar visualizar o número de identificação do banco (BIN) para fins de roteamento, desmascarar apenas os dígitos do BIN para essa função. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
	3.4.1.c Examine as exibições de PAN (por exemplo, na tela, em recibos de papel) para verificar se os PANs estão mascarados quando exibidos e se apenas aqueles com uma necessidade comercial legítima são capazes de ver mais do que o BIN e/ou os últimos quatro dígitos do PAN .	**Definições** Mascaramento não é sinônimo de truncamento e esses termos não podem ser usados de forma intercambiável. O mascaramento refere-se à ocultação de certos dígitos durante a exibição ou impressão, mesmo quando todo o PAN está armazenado em um sistema. Isso é diferente do truncamento, no qual os dígitos truncados são removidos e não podem ser recuperados dentro do sistema. O PAN mascarado pode ser "desmascarado", mas não há "não truncamento" sem recriar o PAN de outra fonte. **Informações Adicionais** Para obter mais informações sobre mascaramento e truncamento, consulte as FAQs do PCI SSC sobre esses tópicos.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
A realocação do PAN para dispositivos de armazenamento não autorizados é uma maneira comum de obter e usar esses dados de maneira fraudulenta.
Métodos para garantir que apenas aqueles com autorização explícita e uma necessidade de negócio legítima pode copiar ou realocar o PAN minimiza o risco de pessoas não autorizadas obterem acesso ao PAN.
Práticas Recomendadas
A cópia e realocação do PAN devem ser feitas apenas para dispositivos de armazenamento que são permitidos e autorizados para aquele indivíduo.
Definições
Uma área de trabalho virtual é um exemplo de tecnologia de acesso remoto.
Os dispositivos de armazenamento incluem, mas não estão limitados a, discos rígidos locais, unidades virtuais, removíveis, mídia eletrônica, unidades de rede e armazenamento em nuvem.
Informações Adicionais
A documentação do fornecedor para a tecnologia de acesso remoto em uso fornecerá informações sobre as configurações do sistema necessárias para implementar este requisito.</td></tr>
<tr><td>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.

Objetivo da Abordagem Personalizada
O PAN não pode ser copiado ou realocado por pessoal não autorizado usando tecnologias de acesso remoto.</td><td>3.4.2.a Examine as políticas e procedimentos documentados e as evidências documentadas dos controles técnicos que evitam a cópia e/ou realocação do PAN em discos rígidos locais ou mídia eletrônica removível ao usar tecnologias de acesso remoto para verificar o seguinte:
• Os controles técnicos evitam que todo o pessoal não especificamente autorizado copie e/ou realoque o PAN.
• Uma lista de pessoal com permissão para copiar e/ou realocar o PAN é mantida, juntamente com a autorização explícita documentada e a necessidade comercial legítima e definida.</td></tr>
<tr><td>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.</td><td>3.4.2.b Examine as configurações das tecnologias de acesso remoto para verificar se os controles técnicos impedem a cópia e/ou realocação do PAN para todo o pessoal, a menos que explicitamente autorizado.</td></tr>
<tr><td></td><td>3.4.2.c Observe os processos e entreviste o pessoal para verificar se apenas o pessoal com autorização explícita documentada e uma necessidade de negócio legítima e definida tem permissão para copiar e/ou realocar o PAN ao usar tecnologias de acesso remoto.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
3.5 O número da conta principal (PAN) é protegido onde quer que seja armazenado.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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. • Truncamento (hash não pode ser usado para substituir o segmento truncado do PAN). Se versões de hash e truncadas do mesmo PAN, ou diferentes formatos de truncamento do mesmo PAN, estiverem presentes em um ambiente, controles adicionais são implementados de forma que as diferentes versões não possam ser correlacionadas para reconstruir o PAN original. • Tokens de índice. • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. `	**3.5.1.a** Examine a documentação sobre o sistema usado para tornar o PAN ilegível, incluindo o fornecedor, o tipo de sistema/processo e os algoritmos de criptografia (se aplicável) para verificar se o PAN é tornado ilegível usando qualquer um dos métodos especificados neste requisito. **3.5.1.b** Examine os repositórios de dados e os registros de auditoria, incluindo os registros de aplicação de pagamento para verificar se o PAN está ilegível usando qualquer um dos métodos especificados neste requisito. **3.5.1.c** Se versões em hash e truncadas do mesmo PAN estiverem presentes no ambiente, examine os controles implementados para verificar se as versões em hash e truncadas não podem	**Objetivo** A remoção do PAN armazenado em texto não criptografado é um controle de defesa em profundidade projetado para proteger os dados se um indivíduo não autorizado obtiver acesso aos dados armazenados, tirando proveito de uma vulnerabilidade ou configuração incorreta do controle de acesso primário de uma entidade. Os sistemas de controle secundários independentes (por exemplo, que regem o acesso e o uso de chaves de criptografia e descriptografia) evitam a falha de um sistema de controle de acesso primário, levando a uma quebra de confidencialidade do PAN armazenado. Se o hash for usado para remover o PAN de texto não criptografado armazenado, um indivíduo mal-intencionado pode derivar facilmente o valor do PAN original correlacionando as versões em hash e truncadas de um determinado PAN. Os controles que

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada O PAN em texto não criptografado não pode ser lido da mídia de armazenamento. **Observações de Aplicabilidade** É um esforço relativamente trivial para um indivíduo mal-intencionado reconstruir os dados do PAN original se ele tiver acesso à versão truncada e o hash de um PAN. 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, registros de auditoria, exceção ou registros de solução de problemas), que devem ser protegidos. Este requisito não impede o uso de arquivos temporários contendo PAN em texto não criptografado durante a criptografia e descriptografia do PAN.	ser correlacionadas para reconstruir o PAN original.	impedem a correlação desses dados ajudarão a garantir que o PAN original permaneça ilegível. **Informações Adicionais** Para obter informações sobre formatos de truncamento e truncamento em geral, consulte as FAQs do PCI SSC sobre o assunto. As fontes de informações sobre tokens de índice incluem: • PCI SSC's Tokenization Product Security Guidelines *(https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)* • *ANSI X9.119-2-2017: Retail Financial Services - Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="5">Objetivo
A remoção do PAN armazenado em texto não criptografado é um controle de defesa em profundidade projetado para proteger os dados se um indivíduo não autorizado obtiver acesso aos dados armazenados, tirando proveito de uma vulnerabilidade ou configuração incorreta do controle de acesso primário de uma entidade.
Os sistemas de controle independentes secundários (por exemplo, que regem o acesso e o uso de chaves de criptografia e descriptografia) evitam a falha de um sistema de controle de acesso primário, levando a uma quebra de confidencialidade do PAN armazenado.
Práticas Recomendadas
Uma função de hashing que incorpora uma chave secreta gerada aleatoriamente fornece resistência a ataques de força bruta e integridade de autenticação secreta.
Informações Adicionais
Algoritmos de hash criptográficos com chave adequados incluem, mas não estão limitados a: HMAC, CMAC e GMAC, com uma força criptográfica efetiva de pelo menos 128 bits (NIST SP 800-131Ar2).
Consulte o seguinte para obter mais informações sobre HMAC, CMAC e GMAC, respectivamente: NIST SP 800-107r1, NIST SP 800-38B, e NIST SP 800-38D.
Consulte NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms §5.3.</td></tr>
<tr><td>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.</td><td>3.5.1.1.a Examine a documentação sobre o método de hashing usado para tornar o PAN ilegível, incluindo o fornecedor, o tipo de sistema/processo e os algoritmos de criptografia (conforme aplicável) para verificar se o método de hashing resulta em hashes criptográficos com chave de todo o PAN, com processos e procedimentos de gerenciamento de chaves associados.</td></tr>
<tr><td rowspan="3">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, registros de auditoria, exceção ou registros de solução de problemas), que devem ser protegidos.
Este requisito não impede o uso de arquivos temporários contendo PAN em texto não criptografado durante a criptograafia e descriptografia do PAN.
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.</td><td>3.5.1.1.b Examine a documentação sobre os procedimentos e processos de gerenciamento de chaves associados aos hashes criptográficos com chave para verificar se as chaves são gerenciadas de acordo com os Requisitos 3.6 e 3.7.</td></tr>
<tr><td>3.5.1.1.c Examine os repositórios de dados para verificar se o PAN está ilegível.</td></tr>
<tr><td>3.5.1.1.d Examine os registros de auditoria, incluindo os registros de aplicativos de pagamento, para verificar se o PAN está ilegível.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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.	**3.5.1.2.a** Examine os processos de criptografia para verificar se a criptografia em nível de disco ou em nível de partição for usada para tornar o PAN ilegível, ela será implementada apenas da seguinte forma: • Em mídia eletrônica removível, **OU** • Se usada para mídia eletrônica não removível, examine os processos de criptografia usados para verificar se o PAN também foi tornado ilegível por meio de outro método que atenda ao Requisito 3.5.1.	**Objetivo** A criptografia em nível de disco e de partição normalmente criptografa todo o disco ou partição usando a mesma chave, com todos os dados descriptografados automaticamente quando o sistema é executado ou quando um usuário autorizado os solicita. Por esse motivo, a criptografia em nível de disco não é apropriada para proteger o PAN armazenado em computadores, laptops, servidores, matrizes de armazenamento ou qualquer outro sistema que forneça descriptografia transparente na autenticação do usuário. **Informações Adicionais** Quando disponível, seguir as diretrizes de práticas recomendadas da indústria e de proteção dos fornecedores pode ajudar a proteger o PAN nesses dispositivos.
Objetivo da Abordagem Personalizada	**3.5.1.2.b** Examine as configurações e/ou a documentação do fornecedor e observe os processos de criptografia para verificar se o sistema está configurado de acordo com a documentação do fornecedor. O resultado é que o disco ou a partição se tornou ilegível.	
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Embora a criptografia de disco 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 em 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 hot-swappable, 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 e gerenciamento de chaves 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 aos dados criptografados são armazenados com segurança.	**3.5.1.3.a** Se a criptografia em nível de disco ou em nível de partição for usada para tornar o PAN ilegível, examine a configuração do sistema e observe o processo de autenticação para verificar se o acesso lógico está implementado de acordo com todos os elementos especificados neste requisito. **3.5.1.3.b** Examine os arquivos contendo os fatores de autenticação (senhas, frases secretas ou chaves criptográficas) e entreviste a equipe para verificar os fatores de autenticação que permitem o acesso a dados não criptografados são armazenadas com segurança e são independentes da autenticação do sistema operacional nativo e dos métodos de controle de acesso.	A criptografia em nível de disco normalmente criptografa todo o disco ou partição usando a mesma chave, com todos os dados descriptografados automaticamente quando o sistema é executado ou quando um usuário autorizado os solicita. Muitas soluções de criptografia de disco interceptam operações de leitura/gravação do sistema operacional e executam as transformações criptográficas apropriadas sem qualquer ação especial do usuário, exceto fornecer uma senha ou frase secreta na inicialização do sistema ou no início de uma sessão. Isso não oferece proteção contra um indivíduo mal-intencionado que já conseguiu obter acesso a uma conta de usuário válida. **Práticas Recomendadas** A criptografia de disco completo ajuda a proteger os dados em caso de perda física de um disco e, portanto, seu melhor uso é limitado apenas a dispositivos de armazenamento de mídia eletrônica removíveis.
Objetivo da Abordagem Personalizada		
As implementações de criptografia de disco são configuradas para exigir autenticação independente e controles de acesso lógico para descriptografia.		
Observações de Aplicabilidade		
As implementações de criptografia de disco ou partição também devem atender a todos os outros requisitos de criptografia e gerenciamento de chaves do PCI DSS.		

Requisitos e Procedimentos de Teste		Diretriz
3.6 As chaves criptográficas usadas para proteger os dados da conta armazenados são protegidas.		
Requisitos da Abordagem Definida **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 custodiantes necessários. • As chaves de criptografia de chave são pelo menos tão fortes quanto às 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. **Objetivo da Abordagem Personalizada** Os processos que protegem as chaves criptográficas usadas para proteger os dados da conta armazenados contra divulgação e uso indevido são definidos e implementados.	**Procedimentos de Teste da Abordagem Definida** **3.6.1** Examine as políticas e procedimentos de gerenciamento de chaves documentados para verificar se os processos para proteger as chaves criptográficas usadas para proteger os dados da conta armazenados contra divulgação e uso indevido são definidos para incluir todos os elementos especificados neste requisito.	**Objetivo** As chaves criptográficas devem ser fortemente protegidas porque aqueles que obtêm acesso poderão descriptografar os dados. **Práticas Recomendadas** Ter um sistema de gerenciamento de chaves centralizado com base nos padrões da indústria é recomendado para o gerenciamento de chaves criptográficas. **Informações Adicionais** Os procedimentos de gerenciamento de chaves da entidade se beneficiarão por meio do alinhamento com os requisitos da indústria. As fontes de informações sobre os ciclos de vida de gerenciamento de chaves criptográficas incluem: • *ISO 11568-1 Banking — Key management (retail) — Part 1*: Principles (especificamente Capítulo 10 e as Partes 2 e 4 referenciadas). • NIST *SP 800-57 Part 1 Revision 5— Recommendation for Key Management, Part 1: General*.

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Este requisito se aplica a chaves usadas para criptografar 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 da conta armazenados 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Manter a documentação atualizada da arquitetura criptográfica permite que uma entidade entenda os algoritmos, protocolos e chaves criptográficas usados para proteger os dados armazenados da conta, bem como os dispositivos que geram, usam e protegem as chaves. Isso permite que uma entidade acompanhe a evolução das ameaças à sua arquitetura e planeje atualizações à medida que o nível de garantia fornecido por diferentes algoritmos e força das chaves muda. A manutenção dessa documentação também permite que uma entidade detecte chaves perdidas ou ausentes ou dispositivos de gerenciamento de chaves e identifique adições não autorizadas à sua arquitetura criptográfica. O uso das mesmas chaves criptográficas em ambientes de produção e teste apresenta o risco de expor a chave se o ambiente de teste não estiver no mesmo nível de segurança que o ambiente de produção. **Práticas Recomendadas** Ter um mecanismo de relatório automatizado pode ajudar na manutenção dos atributos criptográficos.
3.6.1.1 ***Requisito adicional apenas para prestadores de serviços:*** Uma descrição documentada da arquitetura criptográfica é mantida, incluindo: • Detalhes de todos os algoritmos, protocolos e chaves usados para a proteção dos dados da conta armazenados, incluindo força da chave e data de validade. • Impedir o uso das mesmas chaves criptográficas em ambientes de produção e teste. *Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes.* • Descrição do uso da chave para cada chave. • Inventário de quaisquer módulos de segurança de hardware (HSMs), sistemas de gerenciamento de chaves (KMS) e outros dispositivos criptográficos seguros (SCDs) usados para gerenciamento de chaves, incluindo tipo e localização dos dispositivos, conforme descrito no Requisito 12.3.4.	**3.6.1.1** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Entreviste a equipe responsável e examine a documentação para verificar se existe um documento para descrever a arquitetura criptográfica que inclui todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
Detalhes precisos da arquitetura criptográfica são mantidos e disponíveis.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. Em implementações de HSM em nuvem, a responsabilidade pela arquitetura criptográfica de acordo com este requisito será compartilhada entre o provedor de nuvem e o cliente da nuvem. *O item acima (para incluir, na arquitetura de criptografia, que o uso das mesmas chaves criptográficas na produção e teste é impedido) é uma prática recomendada até 31 de março de 2025, após o qual será exigido como parte do Requisito 3.6.1.1 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
3.6.1.2 As chaves secretas e privadas usadas para criptografar/descriptografar os dados da conta armazenados são armazenadas em um (ou mais) dos seguintes formulários o tempo todo: • Criptografadas com uma chave de criptografia de chave que é pelo menos tão forte quanto à 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 principais completos ou partes da chave, de acordo com um método aceito pela indústria.	**3.6.1.2.a** Examine os procedimentos documentados para verificar se está definido que as chaves criptográficas usadas para criptografar/descriptografar os dados da conta armazenados devem existir apenas em um (ou mais) formas especificadas neste requisito. **3.6.1.2.b** Examine as configurações do sistema e os locais de armazenamento de chaves para verificar se as chaves criptográficas usadas para criptografar/descriptografar os dados da conta armazenados existem em um (ou mais) formas especificadas neste requisito. **3.6.1.2.c** Onde quer que as chaves de criptografia sejam usadas, examine as configurações do sistema e os locais de armazenamento de chaves para verificar: • As chaves de criptografia de chave são pelo menos tão fortes quanto às chaves de criptografia de dados que protegem. • As chaves de criptografia de chave são armazenadas separadamente das chaves de criptografia de dados.	**Objetivo** O armazenamento de chaves criptográficas com segurança evita o acesso não autorizado ou desnecessário que pode resultar na exposição dos dados da conta armazenados. Armazenar chaves separadamente significa que elas são armazenadas de forma que, se a localização de uma chave for comprometida, a segunda chave também não será comprometida. **Práticas Recomendadas** Onde as chaves de criptografia de dados são armazenadas em um HSM, o canal de interação do HSM deve ser protegido para evitar a interceptação de operações de criptografia ou decriptografia.
Objetivo da Abordagem Personalizada		
As chaves secretas e privadas são armazenadas de forma segura que impede a recuperação ou acesso não autorizado.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Não é necessário que as chaves públicas sejam armazenadas em uma dessas formas. 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 principais 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 componentes de chave secreta.		
Requisitos da Abordagem Definida **3.6.1.3** O acesso aos componentes da chave criptográfica em texto não criptografado é restrito ao menor número de custodiantes necessários. **Objetivo da Abordagem Personalizada** O acesso aos componentes da chave criptográfica em texto não criptografado é restrito ao pessoal necessário.	**Procedimentos de Teste da Abordagem Definida** **3.6.1.3** Examine as listas de acesso do usuário para verificar se o acesso aos componentes da chave criptográfica em texto não criptografado é restrito ao menor número de custodiantes necessário.	**Objetivo** Restringir o número de pessoas que têm acesso aos componentes da chave criptográfica em texto não criptografado reduz o risco de os dados da conta armazenados serem recuperados ou tornados visíveis por partes não autorizadas. **Práticas Recomendadas** Somente o pessoal com responsabilidades de custódia de chaves definidas (criação, alteração, rotação, distribuição ou manutenção de chaves de criptografia) deve ter acesso aos componentes principais. Idealmente, esse será um número muito pequeno de pessoas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Armazenar quaisquer chaves criptográficas no menor número de locais ajuda uma organização a rastrear e monitorar todos os locais de chaves e minimiza o potencial das chaves serem expostas a pessoas não autorizadas.
3.6.1.4 As chaves criptográficas são armazenadas no menor número possível de locais.	**3.6.1.4** Examine os locais de armazenamento de chaves e observe os processos para verificar se as chaves estão armazenadas no menor número possível de locais.	
Objetivo da Abordagem Personalizada		
As chaves criptográficas são mantidas apenas quando necessário.		

Requisitos e Procedimentos de Teste		Diretriz
3.7 Onde a criptografia é usada para proteger os dados da conta armazenados, os processos e procedimentos de gerenciamento de chave cobrindo todos os aspectos do ciclo de vida da chave são definidos e implementados.		
Requisitos da Abordagem Definida **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 da conta armazenados. **Objetivo da Abordagem Personalizada** Chaves criptográficas fortes são geradas.	**Procedimentos de Teste da Abordagem Definida** **3.7.1.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados para verificar se eles definem a geração de chaves criptográficas fortes. **3.7.1.b** Observe o método de geração de chaves para verificar se as chaves fortes são geradas.	**Objetivo** O uso de chaves criptográficas fortes aumenta significativamente o nível de segurança dos dados criptografados da conta. **Informações Adicionais** Veja as fontes referenciadas em "Geração de Chave Criptográfica no Apêndice G.
Requisitos da Abordagem Definida **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 da conta armazenados. **Objetivo da Abordagem Personalizada** Chaves criptográficas são seguras durante a distribuição.	**Procedimentos de Teste da Abordagem Definida** **3.7.2.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados para verificar se eles definem a distribuição segura de chaves criptográficas. **3.7.2.b** Observe o método de distribuição de chaves para verificar se as chaves são distribuídas com segurança.	**Objetivo** A distribuição ou transporte seguro de chaves criptográficas privadas ou secretas significa que as chaves são distribuídas apenas para custodiantes autorizados, conforme identificado no Requisito 3.6.1.2, e nunca são distribuídas de forma insegura.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O armazenamento de chaves sem proteção adequada pode fornecer acesso a invasores, resultando na descriptografia e exposição dos dados da conta. **Práticas Recomendadas** As chaves de criptografia de dados podem ser protegidas criptografando-as com uma chave de criptografia de chave. As chaves podem ser armazenadas em um módulo de segurança de hardware (HSM). Chaves secretas ou privadas que podem descriptografar dados nunca devem estar presentes no código-fonte.
3.7.3 Políticas e procedimentos de gerenciamento de chaves são implementados para incluir o armazenamento seguro de chaves criptográficas usadas para proteger os dados da conta armazenados.	**3.7.3.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados para verificar se eles definem a distribuição segura de chaves criptográficas.	
	3.7.3.b Observe o método de armazenamento de chaves para verificar se as chaves estão armazenadas com segurança.	
Objetivo da Abordagem Personalizada		
Chaves criptográficas são seguras quando armazenadas.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Alterar as chaves de criptografia quando atingirem o final de seu criptoperíodo é fundamental para minimizar o risco de alguém obter as chaves de criptografia e usá-las para descriptografar os dados. **Definições** Um criptoperíodo é o intervalo de tempo durante o qual uma chave criptográfica pode ser usada para seu propósito definido. Criptoperíodos são frequentemente definidos em termos do período para o qual a chave está ativa e/ou a quantidade de texto cifrado que foi produzido pela chave. As considerações para definir o criptoperíodo incluem, mas não estão limitadas a, a força do algoritmo subjacente, tamanho ou comprimento da chave, risco de comprometimento da chave e a sensibilidade dos dados sendo criptografados. *(continua na página a seguir)*
3.7.4 As políticas e procedimentos de gerenciamento de chaves são implementados para mudanças de chaves criptográficas que atingiram o final de seu criptoperíodo, conforme definido pelo fornecedor do aplicativo associado ou proprietário da chave, e com base nas práticas recomendadas e diretrizes da indústria, incluindo o seguinte: • Um criptoperíodo definido para cada tipo de chave em uso. • Um processo para mudanças de chaves no final do criptoperíodo definido.	**3.7.4.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados para verificar se eles definem mudanças nas chaves criptográficas que alcançaram o fim de seu criptoperíodo e incluem todos os elementos especificados neste requisito.	
	3.7.4.b Entreviste a equipe, examine a documentação e observe os locais de armazenamento das chaves para verificar se as chaves são alteradas no final do(s) criptoperíodo(s) definido(s).	

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada As chaves criptográficas não são usadas além de seu criptoperíodo definido.		**Informações Adicionais** *NIST SP 800-57 Part 1, Revision 5, Section 5.3 Cryptoperiods* - fornece orientação para estabelecer o intervalo de tempo durante o qual uma chave específica é autorizada para uso por entidades legítimas ou as chaves para um determinado sistema permanecerão em vigor. Consulte a Tabela 1 de *SP 800-57* Parte 1 para criptoperíodos sugeridos para diferentes tipos de chave.
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 da conta armazenados, 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 da chave em texto não criptografado deixa a empresa ou a função para a qual o componente da chave era conhecido. • Existe a suspeita ou comprovação de que uma chave está comprometida. Chaves retiradas ou substituídas não são usadas para operações de criptografia.	**3.7.5.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados e verifique se eles definem retirada, substituição ou destruição de chaves de acordo com todos os elementos especificados neste requisito.	Chaves que não são mais necessárias, chaves com integridade enfraquecida e chaves que são conhecidas ou suspeitas de estarem comprometidas devem ser arquivadas, revogadas e/ou destruídas para garantir que as chaves não possam mais ser usadas. Se essas chaves precisarem ser mantidas (por exemplo, para suportar dados criptografados arquivados), elas devem ser fortemente protegidas.
	3.7.5.b Entreviste o pessoal para verificar se os processos são implementados de acordo com todos os elementos especificados neste requisito.	**Práticas Recomendadas** As chaves criptográficas arquivadas devem ser usadas apenas para fins de descriptografia/verificação. A solução de criptografia deve fornecer e facilitar um processo para substituir as chaves que devem ser substituídas ou que são conhecidas ou suspeitas de estarem comprometidas. Além disso, todas as chaves que são conhecidas ou suspeitas de estarem comprometidas devem ser gerenciadas de acordo com o plano de resposta a incidentes da entidade no Requisito 12.10.1.
Objetivo da Abordagem Personalizada As chaves são removidas do uso ativo quando há suspeita ou conhecimento de que a integridade da chave está enfraquecida.		

Requisitos e Procedimentos de Teste		Diretriz
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).		**Informações Adicionais** As práticas recomendadas da indústria para o arquivamento de chaves retiradas são descritas no *NIST SP 800-57 Part 1, Revision 5, Section 8.3.1,* e incluem a manutenção do arquivamento com um terceiro confiável e o armazenamento de informações de chaves arquivadas separadamente dos dados operacionais.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O conhecimento dividido e o controle duplo de chaves são usados para eliminar a possibilidade de uma única pessoa ter acesso a toda a chave e, portanto, ter acesso não autorizado aos dados. **Definições** O conhecimento dividido é um método em que duas ou mais pessoas separadamente possuem componentes de chave, onde cada pessoa conhece apenas seu próprio componente de chave e os componentes de chaves individuais não transmitem nenhum conhecimento de outros componentes ou da chave criptográfica original. O controle duplo requer duas ou mais pessoas para autenticar o uso de uma chave criptográfica ou executar uma função de gerenciamento de chave. Nenhuma pessoa pode acessar ou usar o fator de autenticação (por exemplo, a senha, PIN ou chave) de outra. **Práticas Recomendadas** Onde componentes de chave ou compartilhamentos de chaves são usados, os procedimentos devem garantir que nenhum custodiante único tenha acesso a compartilhamentos ou componentes de chaves suficientes para reconstruir a chave criptográfica. Por exemplo, em um esquema m-de-n (por exemplo, Shamir), onde apenas dois dos três componentes são necessários para reconstruir a chave criptográfica, um custodiante não deve ter conhecimento atual ou prévio de mais de um componente. Se um custodiante foi previamente atribuído ao componente A, que foi então reatribuído, o custodiante não deve ser atribuído ao componente B ou C, pois isso daria ao custodiante o conhecimento de dois componentes e a capacidade de recriar a chave. *(continua na página a seguir)*
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.	**3.7.6.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados e verifique se eles definem o uso de conhecimento dividido e controle duplo.	
	3.7.6.b Entreviste a equipe e/ou observe os processos para verificar se as chaves manuais em texto não criptografado são gerenciadas com conhecimento dividido e controle duplo.	
Objetivo da Abordagem Personalizada		
As chaves privadas ou secretas em texto não criptografado não podem ser conhecidas por ninguém. As operações que envolvem chaves em texto não criptografado não podem ser realizadas por uma única pessoa.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Esse controle é aplicável para operações manuais de gerenciamento de chaves ou onde o gerenciamento de chaves não é controlado pelo produto de criptografia. Uma chave criptográfica que é dividida simplesmente em duas partes não atende a esse requisito. Chaves secretas ou privadas armazenadas como componentes de 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 componentes de chave secreta.		**Exemplos** As operações de gerenciamento de chaves que podem ser executadas manualmente incluem, mas não estão limitadas a, geração, transmissão, carregamento, armazenamento e destruição de chaves. **Informações Adicionais** Os padrões da indústria para o gerenciamento de componentes de chave incluem: • *NIST SP 800-57* Part 2, Revision 1 -- Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [4.6 Keying Material Distribution] • *ISO 11568-2 Banking — Key management (retail) — Part 2*: Symmetric ciphers, their key management and life cycle [4.7.2.3 Key components and 4.9.3 Key components] • *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [especially 4.1.4 Key installation].

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **3.7.7** As políticas e procedimentos de gerenciamento de chaves são implementados para incluir a prevenção da substituição não autorizada de chaves criptográficas. **Objetivo da Abordagem Personalizada** As chaves criptográficas não podem ser substituídas por pessoal não autorizado.	**Procedimentos de Teste da Abordagem Definida** **3.7.7.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados e verifique se eles definem a prevenção de substituição não autorizada de chaves criptográficas. **3.7.7.b** Entreviste o pessoal e/ou observe os processos para verificar se a substituição não autorizada de chaves é evitada.	**Objetivo** Se um invasor for capaz de substituir a chave de uma entidade por uma chave que o invasor conhece, este será capaz de descriptografar todos os dados criptografados com essa chave. **Práticas Recomendadas** A solução de criptografia não deve permitir ou aceitar a substituição de chaves de fontes não autorizadas ou processos inesperados. Os controles devem incluir a garantia de que os indivíduos com acesso aos componentes de chave ou compartilhamentos não tenham acesso a outros componentes ou compartilhamentos que formam o limite necessário para derivar a chave.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os custodiantes das chaves estão bem informados sobre suas responsabilidades em relação às operações criptográficas e podem ter acesso à assistência e orientação quando necessário.	**Procedimentos de Teste da Abordagem Definida** **3.7.8.a** Examine as políticas e procedimentos de gerenciamento de chaves documentados para chaves usadas para proteção de dados da conta armazenados e verifique se eles definem reconhecimentos para os custodiantes de chave de acordo com todos os elementos especificados neste requisito. **3.7.8.b** Examine a documentação ou outra evidência que mostre que os custodiantes de chave forneceram reconhecimentos de acordo com todos os elementos especificados neste requisito.	**Objetivo** Esse processo ajudará a garantir que os indivíduos que atuam como custodiante das chaves se comprometam com a função de custodiante das chaves e compreendam e aceitem as responsabilidades. Uma reafirmação anual pode ajudar a lembrar os principais custodiantes de suas responsabilidades. **Informações Adicionais** A orientação da indústria para os custodiantes de chave e suas funções e responsabilidades incluem: • *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* [5. Roles and Responsibilities (especially) for Key Custodians] • *ISO 11568-1 Banking -- Key management (retail) -- Part 1*: Principles [5 Principles of key management (especially b)]

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
3.7.9 ***Requisito adicional apenas para prestadores de serviços:*** Quando um prestador de serviços compartilha chaves criptográficas com seus clientes para transmissão ou armazenamento de dados de contas, orientações sobre transmissão segura, armazenamento e atualização de tais chaves são documentadas e distribuídas aos clientes dos prestadores de serviços.	**3.7.9** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Se o prestador de serviços compartilhar chaves criptográficas com seus clientes para transmissão ou armazenamento de dados da conta, examine a documentação que o prestador de serviços fornece a seus clientes para verificar se inclui orientações sobre como transmitir, armazenar e atualizar com segurança as chaves dos clientes de acordo com todos os elementos especificados nos Requisitos 3.7.1 a 3.7.8 acima.	Fornecer orientação aos clientes sobre como transmitir, armazenar e atualizar chaves criptográficas com segurança pode ajudar a evitar que as chaves sejam mal gerenciadas ou divulgadas a entidades não autorizadas. **Informações Adicionais** Vários padrões da indústria para gerenciamento de chaves são citados acima nas Diretrizes para Requisitos 3.7.1-3.7.8.
Objetivo da Abordagem Personalizada		
Os clientes recebem orientações de gerenciamento de chaves adequadas sempre que recebem chaves criptográficas compartilhadas.		
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

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

Seções	
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 documentados.
4.2	O PAN é protegido com criptografia forte durante a transmissão.

Visão Geral

O uso de criptografia forte fornece maior segurança na preservação da confidencialidade, integridade e não repúdio dos dados.

Para proteger contra comprometimento, o PAN deve ser criptografado durante a transmissão em redes que são facilmente acessadas por indivíduos mal-intencionados, incluindo redes públicas e não confiáveis. Redes sem fio mal configuradas e vulnerabilidades em protocolos legados de criptografia e autenticação continuam a ser visados por indivíduos mal-intencionados com o objetivo de explorar essas vulnerabilidades para obter acesso privilegiado aos ambientes de dados do titular do cartão (CDE). Quaisquer transmissões de dados do titular do cartão pela(s) rede(s) interna(s) de uma entidade irão naturalmente trazer essa rede para o escopo do PCI DSS, uma vez que essa rede armazena, processa ou transmite os dados do titular do cartão. Qualquer uma dessas redes deve ser avaliada e analisada em relação aos requisitos aplicáveis do PCI DSS.

O Requisito 4 se aplica a transmissões de PAN, a menos que seja especificamente solicitado em um requisito individual.

As transmissões PAN podem ser protegidas criptografando os dados antes de serem transmitidos ou criptografando a sessão pela qual os dados são transmitidos, ou ambos. Embora não seja necessário que uma criptografia forte seja aplicada tanto no nível de dados quanto no nível de sessão, ela é recomendada.

Consulte o Apêndice G para obter as definições de “Criptografia Forte” e outros termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
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 documentados.		
Requisitos da Abordagem Definida **4.1.1** Todas as políticas e processos operacionais identificados no Requisito 4 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 4 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **4.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 4 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 4.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 4. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 4, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política. Políticas e procedimentos, incluindo atualizações, são comunicados ativamente a todo o pessoal afetado e são apoiados por procedimentos operacionais que descrevem como realizar as atividades.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer.
Práticas Recomendadas
As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados.
Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas.
Exemplos
Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).</td></tr>
<tr><td>4.1.2 As funções e responsabilidades para a execução de atividades no Requisito 4 são documentadas, atribuídas e compreendidas.</td><td>4.1.2.a Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 4 estão documentadas e atribuídas.</td></tr>
<tr><td rowspan="2"></td><td>4.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 4 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada</td></tr>
<tr><td>As responsabilidades do dia a dia para realizar todas as atividades no Requisito 4 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.</td><td></td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
4.2 O PAN é protegido com criptografia forte durante a transmissão		
Requisitos da Abordagem Definida **4.2.1** Criptografia forte e protocolos de segurança são implementados da seguinte forma para proteger o PAN durante a transmissão em redes públicas abertas: • Somente chaves e certificados confiáveis são aceitos. • 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. **Objetivo da Abordagem Personalizada** O PAN em texto não criptografado não pode ser lido ou interceptado em nenhuma transmissão em redes públicas abertas.	**Procedimentos de Teste da Abordagem Definida** **4.2.1.a** Examine as políticas e procedimentos documentados e entreviste o pessoal para verificar se os processos estão definidos para incluir todos os elementos especificados neste requisito. **4.2.1.b** Examine as configurações do sistema para verificar se a criptografia forte e os protocolos de segurança estão implementados de acordo com todos os elementos especificados neste requisito. **4.2.1.c** Examine as transmissões de dados do titular do cartão para verificar se todo o PAN está criptografado com criptografia forte quando é transmitido em redes públicas abertas. **4.2.1.d** Examine as configurações do sistema para verificar se as chaves e/ou certificados que não podem ser verificados como confiáveis foram rejeitados.	**Objetivo** As informações confidenciais devem ser criptografadas durante a transmissão em redes públicas porque é fácil e comum para um indivíduo mal-intencionado interceptar e/ou desviar dados durante o trânsito. **Práticas Recomendadas** Os diagramas de rede e de fluxo de dados definidos no Requisito 1 são recursos úteis para identificar todos os pontos de conexão onde os dados da conta são transmitidos ou recebidos em redes públicas abertas. Embora não seja obrigatório, é considerada uma boa prática que as entidades também criptografem o PAN em suas redes internas e que as entidades estabeleçam novas implementações de rede com comunicações criptografadas. As transmissões do PAN podem ser protegidas criptografando os dados antes de serem transmitidos ou criptografando a sessão pela qual os dados são transmitidos, ou ambos. Embora não seja necessário que uma criptografia forte seja aplicada tanto no nível de dados quanto no nível de sessão, ela é altamente recomendada. Se criptografadas no nível dos dados, as chaves criptográficas usadas para proteger os dados podem ser gerenciadas de acordo com os Requisitos 3.6 e 3.7. Se os dados forem criptografados no nível da sessão, os custodiantes de chave designados devem ser responsáveis pelo gerenciamento das chaves de transmissão e certificados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Pode haver ocorrências em que uma entidade receba dados do titular do cartão não solicitados por meio de um canal de comunicação inseguro que não foi criado com o objetivo de receber 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 implementar medidas para evitar que o canal seja usado para os dados do titular do cartão. Um certificado autoassinado também pode ser aceitável se o certificado for emitido por uma CA interna 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. Observe que os certificados autoassinados em que o campo Distinguished Name (DN) nos campos “emitido por” e “emitido para” é o mesmo não são aceitáveis. *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 o qual será exigido como parte do Requisito 4.2.1 e deve ser totalmente considerado durante uma avaliação do PCI DSS.*		Algumas implementações de protocolo (como SSL, SSH v1.0 e TLS antigo) têm vulnerabilidades conhecidas que um invasor pode usar para obter acesso aos dados em texto não criptografado. É essencial que as entidades mantenham o conhecimento das datas de descontinuação definidas pela indústria para os conjuntos de criptografia que estão usando e estejam preparadas para migrar para versões ou protocolos mais recentes quando os mais antigos não forem mais considerados seguros. Verificar se os certificados são confiáveis ajuda a garantir a integridade da conexão segura. Para ser considerado confiável, um certificado deve ser emitido de uma fonte confiável, como uma autoridade de certificação (CA) confiável, e não deve ter expirado. Listas de revogação de certificado (CRLs) atualizadas ou protocolo de status de certificado online (OCSP) podem ser usados para validar certificados. As técnicas para validar certificados podem incluir a fixação de certificado e chave pública, em que o certificado confiável ou uma chave pública é fixada durante o desenvolvimento ou em seu primeiro uso. As entidades também podem confirmar com os desenvolvedores ou revisar o código-fonte para garantir que os clientes e servidores rejeitem as conexões se o certificado for inválido. Para certificados TLS baseados em navegador, a confiança do certificado geralmente pode ser verificada clicando no ícone de cadeado que aparece ao lado da barra de endereço. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		Exemplos As redes abertas e públicas incluem, mas não se limitam a: • Internet e • Tecnologias sem fio, incluindo Wi-Fi, Bluetooth, tecnologias de celular e comunicações por satélite. **Informações Adicionais** As recomendações do fornecedor e as práticas recomendadas da indústria podem ser consultadas para obter informações sobre a força de criptografia adequada, específica para a metodologia de criptografia em uso. Para obter mais informações sobre criptografia forte e protocolos seguros, consulte os padrões da indústria e as práticas recomendadas, como a *NIST SP 800-52* e *SP 800-57.* Para obter mais informações sobre chaves e certificados confiáveis, consulte a *NIST Cybersecurity Practice Guide Special Publication 1800-16*, *Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.*

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O inventário de chaves confiáveis ajuda a entidade a controlar os algoritmos, protocolos, força da chave, custodiantes da chave e datas de expiração da chave. Isso permite que a entidade responda rapidamente às vulnerabilidades descobertas no software de criptografia, certificados e algoritmos criptográficos. **Práticas Recomendadas** Para certificados, o inventário deve incluir a CA de emissão e a data de expiração da certificação.
4.2.1.1 Um inventário das chaves e certificados confiáveis da entidade usados para proteger o PAN durante a transmissão é mantido.	**4.2.1.1.a** Examine as políticas e procedimentos documentados para verificar se os processos estão definidos para a entidade manter um inventário de suas chaves e certificados confiáveis.	
	4.2.1.1.b Examine o inventário de chaves e certificados confiáveis para verificar se está atualizado.	
Objetivo da Abordagem Personalizada		
Todas as chaves e certificados usados para proteger o PAN durante a transmissão são identificados e confirmados como 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** O PAN em texto não criptografado não pode ser lido ou interceptado nas transmissões de rede wireless.	**Procedimentos de Teste da Abordagem Definida** **4.2.1.2** Examine as configurações do sistema para verificar se as redes wireless que transmitem o PAN ou conectadas ao CDE usam as práticas recomendadas da indústria para implementar criptografia forte para autenticação e transmissão.	**Objetivo** Como as redes wireless não exigem mídia física para se conectar, é importante estabelecer controles que limitem quem pode se conectar e quais protocolos de transmissão serão usados. Usuários mal-intencionados usam ferramentas gratuitas e amplamente disponíveis para espionar comunicações wireless. O uso de criptografia forte pode ajudar a limitar a divulgação de informações confidenciais em redes wireless. As redes wireless apresentam riscos exclusivos para uma organização; portanto, elas devem ser identificadas e protegidas de acordo com os requisitos da indústria. Uma criptografia forte para autenticação e transmissão de PAN é necessária para evitar que usuários mal-intencionados obtenham acesso à rede wireless ou utilizem redes wireless para acessar outras redes internas ou dados. **Práticas Recomendadas** As redes wireless não devem permitir falhas ou redução para um protocolo inseguro ou menor força de criptografia que não atenda ao objetivo de criptografia forte. **Informações Adicionais** Revise a documentação específica do fornecedor para obter mais detalhes sobre a escolha de protocolos, configurações e definições relacionadas à criptografia.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **4.2.2** O PAN é protegido por criptografia forte sempre que enviado por meio de tecnologias de mensagens do usuário final.	**Procedimentos de Teste da Abordagem Definida** **4.2.2.a** Examine as políticas e procedimentos documentados para verificar se os processos são definidos para proteger o PAN com criptografia forte, sempre que enviado por meio de tecnologias de mensagens do usuário final.	**Objetivo** As tecnologias de mensagens do usuário final normalmente podem ser facilmente interceptadas pela detecção de pacotes durante a entrega nas redes internas e públicas. **Práticas Recomendadas** O uso da tecnologia de mensagens do usuário final para enviar o PAN deve ser considerado apenas onde houver uma necessidade comercial definida. **Exemplos** E-mail, mensagens instantâneas, SMS e bate-papo são exemplos do tipo de tecnologia de mensagens do usuário final a que esse requisito se refere.
Objetivo da Abordagem Personalizada O PAN em texto não criptografado não pode ser lido ou interceptado nas transmissões usando tecnologias de mensagens do usuário final.	**4.2.2.b** Examine as configurações do sistema e a documentação do fornecedor para verificar se o PAN é protegido por criptografia forte sempre que é enviado por meio de tecnologias de mensagens do usuário final.	
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

Seções	
5.1	Processos e mecanismos para proteger todos os sistemas e redes de software malicioso são definidos e compreendidos.
5.2	O software malicioso (malware) é evitado ou detectado e resolvido.
5.3	Os mecanismos e processos antimalware são ativos, mantidos e monitorados.
5.4	Os mecanismos antiphishing protegem os usuários contra ataques de phishing.

Visão Geral

Software malicioso (malware) é um software ou firmware projetado para se infiltrar ou danificar um sistema de computador sem o conhecimento ou consentimento do proprietário, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional do proprietário.

Os exemplos incluem vírus, worms, cavalos de Tróia, spyware, ransomware, keyloggers e rootkits, código malicioso, scripts e links.

O malware pode entrar na rede durante muitas atividades aprovadas pela empresa, incluindo e-mail de funcionários (por exemplo, por meio de phishing) e uso da Internet, computadores móveis e dispositivos de armazenamento, resultando na exploração de vulnerabilidades do sistema.

Usar soluções antimalware que abordam todos os tipos de malware ajuda a proteger os sistemas contra ameaças de malware atuais e em evolução.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
5.1 Processos e mecanismos para proteger todos os sistemas e redes de software malicioso são definidos e compreendidos.		
Requisitos da Abordagem Definida **5.1.1** Todas as políticas e processos operacionais identificados no Requisito 5 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 5 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **5.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 5 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 5.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 5. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 5, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, as redes e os sistemas podem não ser protegidos adequadamente contra malware. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
5.1.2 As funções e responsabilidades para a execução de atividades no Requisito 5 são documentadas, atribuídas e compreendidas.	**5.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 5 estão documentadas e atribuídas.	
	5.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 5 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 5 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
5.2 O software malicioso (malware) é evitado ou detectado e corrigido.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Há um fluxo constante de ataques que visam vulnerabilidades recém-descobertas em sistemas antes considerados seguros. Sem uma solução antimalware que seja atualizada regularmente, novas formas de malware podem ser usadas para atacar sistemas, desabilitar uma rede ou comprometer dados. **Práticas Recomendadas** É benéfico para as entidades estarem cientes dos ataques de "dia zero" (aqueles que exploram uma vulnerabilidade anteriormente desconhecida) e considerar soluções que se concentram em características comportamentais e alertarão e reagirão a comportamentos inesperados. **Definições** Os componentes de sistema conhecidos por serem afetados por malware têm explorações de malware (*exploits*) ativas disponíveis no mundo real (não apenas explorações teóricas).
5.2.1 Uma(s) solução(ões) antimalware são implantadas em todos os componentes de sistema, exceto para aqueles componentes de sistema identificados em avaliações periódicas de acordo com o Requisito 5.2.3 que conclui que os componentes de sistema não correm risco de malware.	**5.2.1.a** Examine os componentes de sistema para verificar se a(s) solução(ões) antimalware está(ão) implantada(s) em todos os componentes de sistema, exceto para aqueles determinados como não correndo risco de malware com base em avaliações periódicas de acordo com o Requisito 5.2.3.	
	5.2.1.b Para todos os componentes de sistema sem uma solução antimalware, examine as avaliações periódicas para verificar se o componente foi avaliado e a avaliação conclui que o componente não corre risco de malware.	
Objetivo da Abordagem Personalizada		
Mecanismos automatizados são implementados para evitar que os sistemas se tornem vetores de ataque para malware.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** É importante se proteger contra todos os tipos e formas de malware para evitar o acesso não autorizado. **Práticas Recomendadas** As soluções antimalware podem incluir uma combinação de controles baseados em rede, controles baseados em host e soluções de segurança de endpoint. Além de ferramentas baseadas em assinatura, os recursos usados por soluções antimalware modernas incluem sandbox, controles de escalonamento de privilégios e aprendizado de máquina. As técnicas de solução incluem impedir que malware entre na rede, bem como remover ou conter malware que entra na rede. **Exemplos** Os tipos de malware incluem, mas não estão limitados a, vírus, cavalos de Troia, worms, spyware, ransomware, keyloggers, rootkits, código malicioso, scripts e links.
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.	**5.2.2** Examine a documentação do fornecedor e as configurações da(s) solução(ões) antimalware para verificar se a solução: • Detecta *todos os tipos conhecidos de malware.* • Remove*, bloqueia ou contém todos os tipos conhecidos de malware.*	
Objetivo da Abordagem Personalizada		
O malware não pode ser executado ou infectar outros componentes de sistema.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
5.2.3 Todos os componentes de sistema que não apresentam risco de malware são avaliados periodicamente para incluir o seguinte: • Uma lista documentada de todos os componentes de sistema sem risco de malware. • Identificação e avaliação de ameaças de malware em evolução para esses componentes de sistema. • Confirmação se tais componentes de sistema continuam a não exigir proteção antimalware.	**5.2.3.a** Examine as políticas e procedimentos documentados para verificar se um processo está definido para avaliações periódicas de qualquer componente de sistema que não corre risco de malware que inclui todos os elementos especificados neste requisito. **5.2.3.b** Entreviste o pessoal para verificar se as avaliações incluem todos os elementos especificados neste requisito. **5.2.3.c** Examine a lista de componentes de sistema identificados como sem risco de malware e compare com os componentes de sistema sem uma solução antimalware implantada de acordo com o Requisito 5.2.1 para verificar se os componentes de sistema correspondem a ambos os requisitos.	Certos sistemas, em um determinado momento, podem não ser comumente visados ou afetados por malware. No entanto, as tendências da indústria para malware podem mudar rapidamente, por isso é importante para as organizações estarem cientes de novos malwares que podem afetar seus sistemas - por exemplo, monitorando avisos de segurança de fornecedores e fóruns de antimalware para determinar se seus sistemas podem estar sendo afetados pela ameaça de malware novo e em evolução. **Práticas Recomendadas** Se uma entidade determinar que um determinado sistema não é suscetível a qualquer malware, a determinação deve ser apoiada por evidências da indústria, recursos do fornecedor e práticas recomendadas. As etapas a seguir podem ajudar as entidades durante suas avaliações periódicas: • Identificação de todos os tipos de sistema previamente determinados para não exigir proteção contra malware. • Revisão dos alertas e avisos de vulnerabilidade da indústria para determinar se existem novas ameaças para qualquer sistema identificado. • Uma conclusão documentada sobre se os tipos de *sistema* permanecem não suscetíveis a malware. • Uma estratégia para adicionar proteção contra malware para qualquer tipo de sistema para o qual a proteção contra malware se tornou necessária. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
A entidade mantém consciência da evolução das ameaças de malware para garantir que quaisquer sistemas não protegidos contra malware não corram o risco de infecção.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Os componentes de sistema cobertos por este requisito são aqueles para os quais não há solução antimalware implantada de acordo com o Requisito 5.2.1.		Tendências em malware devem ser incluídas na identificação de novas vulnerabilidades de segurança no Requisito 6.3.1, e métodos para lidar com novas tendências devem ser incorporados aos padrões de configuração da entidade e mecanismos de proteção conforme necessário.
Requisitos da Abordagem Definida **5.2.3.1** A frequência das avaliações periódicas dos componentes de 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.	**Procedimentos de Teste da Abordagem Definida** **5.2.3.1.a** Examine a análise de risco direcionada da entidade para a frequência das avaliações periódicas dos componentes de sistema identificados como sem risco de malware para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	**Objetivo** As entidades determinam o período ideal para realizar a avaliação com base em critérios como a complexidade do ambiente de cada entidade e o número de tipos de sistemas que devem ser avaliados.
	5.2.3.1.b Examine os resultados documentados das avaliações periódicas dos componentes de sistema identificados como sem risco para malware e entreviste o pessoal para verificar se as avaliações são realizadas na frequência definida na análise de risco direcionada da entidade realizada para este requisito.	
Objetivo da Abordagem Personalizada Os sistemas que não apresentam risco de malware são reavaliados com uma frequência que aborda o risco da entidade.		
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.*		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td colspan="3">5.3 Os mecanismos e processos antimalware são ativos, mantidos e monitorados.</td></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
Para que uma solução antimalware permaneça eficaz, ela precisa ter as últimas atualizações de segurança, assinaturas, mecanismos de análise de ameaças e quaisquer outras proteções de malware das quais a solução dependa.
Ter um processo de atualização automatizado evita sobrecarregar os usuários finais com a responsabilidade de instalar manualmente as atualizações e oferece maior garantia de que os mecanismos de proteção antimalware sejam atualizados o mais rápido possível após o lançamento de uma atualização.
Práticas Recomendadas
Os mecanismos antimalware devem ser atualizados através de uma fonte confiável assim que possível após uma atualização estar disponível. Usar uma fonte comum confiável para distribuir atualizações aos sistemas do usuário final ajuda a garantir a integridade e a consistência da arquitetura da solução.
As atualizações podem ser baixadas automaticamente para um local central - por exemplo, para permitir o teste - antes de serem implantadas em componentes de sistema individuais.</td></tr>
<tr><td>5.3.1 As soluções antimalware são mantidas atualizadas por meio de atualizações automáticas.</td><td>5.3.1.a Examine as configurações das soluções antimalware, incluindo qualquer instalação mestre do software, para verificar se a solução está configurada para realizar atualizações automáticas.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
Os mecanismos antimalware podem detectar e resolver as ameaças de malware mais recentes.</td><td>5.3.1.b Examine os componentes de sistema e registros, para verificar se as soluções e definições antimalware estão atualizadas e foram prontamente implantadas</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
5.3.2 A(s) solução(ões) antimalware: • Executa varreduras periódicas e varreduras ativas ou em tempo real. **OU** • Executa análises comportamentais contínuas de sistemas ou processos.	**5.3.2.a** Examine as configurações da solução(ões) antimalware, incluindo qualquer instalação mestre do software, para verificar se a(s) solução(ões) está(ão) configurada(s) para executar pelo menos um dos elementos especificados neste requisito.	**Objetivo** As varreduras periódicas podem identificar malware que está presente, mas atualmente inativo, no ambiente. Alguns malwares, como malware de dia zero, podem entrar em um ambiente antes que a solução de varredura seja capaz de detectá-lo. A execução de varreduras periódicas regulares ou análise comportamental contínua de sistemas ou processos ajuda a garantir que malware anteriormente indetectável possa ser identificado, removido e investigado para determinar como obteve acesso ao ambiente. **Práticas Recomendadas** O uso de uma combinação de varreduras periódicas (programadas e sob demanda) e varreduras ativas em tempo real (no acesso) ajuda a garantir que o malware residente em elementos estáticos e dinâmicos do CDE seja corrigido. Os usuários também devem ser capazes de executar varreduras sob demanda em seus sistemas se uma atividade suspeita for detectada - isso pode ser útil na detecção precoce de malware. As verificações devem incluir todo o sistema de arquivos, incluindo todos os discos, memória e arquivos de inicialização e registros de inicialização (na reinicialização do sistema) para detectar todos os malwares na execução do arquivo, incluindo qualquer software que possa residir em um sistema, mas não esteja ativo no momento. O escopo da varredura deve incluir todos os sistemas e softwares no CDE, incluindo aqueles que são frequentemente esquecidos, como servidores de e-mail, navegadores da web e software de mensagens instantâneas. *(continua na página a seguir)*
	5.3.2.b Examine os componentes de sistema, incluindo todos os tipos de sistema operacional identificados como de risco para malware, para verificar se a(s) solução(ões) está(ão) habilitada(s) de acordo com pelo menos um dos elementos especificados neste requisito.	
	5.3.2.c Examine os registros e os resultados da varredura para verificar se a(s) solução(ões) está(ão) habilitada(s) de acordo com pelo menos um dos elementos especificados neste requisito.	

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada O malware não consegue completar a execução.		**Definições** A varredura ativa, ou em tempo real, verifica os arquivos em busca de malware em qualquer tentativa de abrir, fechar, renomear ou interagir de outra forma com um arquivo, evitando que o malware seja ativado.
Requisitos da Abordagem Definida **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.	**Procedimentos de Teste da Abordagem Definida** **5.3.2.1.a** Examine a análise de risco direcionada da entidade para a frequência de varreduras periódicas de malware para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1. **5.3.2.1.b** Examine os resultados documentados das varreduras de malware periódicas e entreviste a equipe para verificar se as varreduras são realizadas na frequência definida na análise de risco direcionada da entidade realizada para este requisito.	**Objetivo** As entidades podem determinar o período ideal para realizar varreduras periódicas com base em sua própria avaliação dos riscos apresentados a seus ambientes.
Objetivo da Abordagem Personalizada As varreduras pela solução de malware são realizadas com uma frequência que aborda o risco da entidade.		
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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
5.3.3 Para mídia eletrônica removível, a solução(ões) antimalware: • Executa varreduras automáticas quando a mídia é inserida, conectada ou montada logicamente, **OU** • Executa análises comportamentais contínuas de sistemas ou processos quando a mídia é inserida, conectada ou montada logicamente.	**5.3.3.a** Examine as configurações da solução(ões) antimalware para verificar se, para mídia eletrônica removível, a solução está configurada para executar pelo menos um dos elementos especificados neste requisito.	Dispositivos de mídia portáteis são frequentemente esquecidos como um método de entrada de malware. Os invasores geralmente pré-carregam malware em dispositivos portáteis, como unidades USB e flash; conectar um dispositivo infectado a um computador aciona o malware, introduzindo novas ameaças no ambiente.
	5.3.3.b Examine os componentes de sistema com mídia eletrônica removível conectada para verificar se a(s) solução(ões) está(ão) habilitada(s) de acordo com pelo menos um dos elementos conforme especificado neste requisito.	
Objetivo da Abordagem Personalizada	**5.3.3.c** Examine os registros e os resultados da varredura para verificar se a(s) solução(ões) está(ão) habilitada(s) de acordo com pelo menos um dos elementos especificados neste requisito.	
O malware não pode ser introduzido nos componentes de sistema por meio de mídia removível externa.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** É importante rastrear a eficácia dos mecanismos antimalware - por exemplo, confirmando se as atualizações e varreduras estão sendo realizadas conforme o esperado e se o malware foi identificado e corrigido. Os registros de auditoria também permitem que uma entidade determine como o malware entrou no ambiente e rastreie sua atividade quando dentro da rede da entidade.
5.3.4 Os registros de auditoria das soluções antimalware estão ativados e retidos de acordo com o Requisito 10.5.1.	**5.3.4** Examine as configurações da(s) solução(ões) antimalware para verificar se os registros estão ativados e retidos de acordo com o Requisito 10.5.1.	
Objetivo da Abordagem Personalizada		
Registros históricos de ações antimalware estão imediatamente disponíveis e retidos por pelo menos 12 meses.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** É importante que os mecanismos de defesa estejam sempre em execução para que o malware seja detectado em tempo real. O início e a interrupção ad-hoc de soluções antimalware podem permitir que o malware se propague sem verificação e sem detecção. **Práticas Recomendadas** Onde houver uma necessidade legítima de desativar temporariamente a proteção antimalware de um sistema - por exemplo, para apoiar uma atividade de manutenção específica ou investigação de um problema técnico - a razão para tomar tal ação deve ser entendida e aprovada por um representante da gestão apropriado. Qualquer desativação ou alteração dos mecanismos antimalware, incluindo nos próprios dispositivos dos administradores, deve ser realizada por pessoal autorizado. É reconhecido que os administradores têm privilégios que podem permitir que desabilitem os antimalware em seus próprios computadores, mas deve haver mecanismos de alerta quando esses controles são desabilitados e o acompanhamento que ocorre para garantir que os processos sejam seguidos. **Exemplos** As medidas de segurança adicionais que podem precisar ser implementadas para o período durante o qual a proteção antimalware não está ativa incluem desconectar o sistema desprotegido da Internet enquanto a proteção antimalware está desabilitada e executar uma verificação completa assim que for reativada.
5.3.5 Os mecanismos antimalware não podem ser desabilitados ou alterados pelos usuários, a menos que especificamente documentados e autorizados pela administração, caso a caso, por um período de tempo limitado.	**5.3.5.a** Examine as configurações do antimalware para verificar se os mecanismos antimalware não podem ser desabilitados ou alterados pelos usuários.	
Objetivo da Abordagem Personalizada Os mecanismos antimalware não podem ser modificados por pessoal não autorizado.	**5.3.5.b** Entreviste a equipe responsável e observe os processos para verificar se todas as solicitações para desabilitar ou alterar os mecanismos antimalware são especificamente documentadas e autorizadas pela administração, caso a caso, por um período de tempo limitado.	
Observações de Aplicabilidade As soluções antimalware podem ser temporariamente desativadas apenas se houver necessidade técnica legítima, conforme autorizado pela administração de acordo com o caso. A proteção antimalware precisa ser desabilitada para um propósito específico, e deverá ser formalmente autorizada. Também podem ser necessárias medidas de segurança adicionais para o período durante o qual esses controles de segurança não estão ativos.		

Requisitos e Procedimentos de Teste		Diretriz
5.4 Os mecanismos antiphishing protegem os usuários contra ataques de phishing.		
Requisitos da Abordagem Definida **5.4.1** Processos e mecanismos automatizados estão em vigor para detectar e proteger o pessoal contra ataques de phishing. **Objetivo da Abordagem Personalizada** Existem mecanismos para proteger e reduzir o risco representado por ataques de phishing. **Observações de Aplicabilidade** Este requisito se aplica ao mecanismo automatizado. Não se pretende que os sistemas e serviços que fornecem tais mecanismos automatizados (como servidores de e-mail) sejam incluídos no escopo do PCI DSS. O foco deste requisito é proteger a equipe com acesso aos componentes de 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.*	**Procedimentos de Teste da Abordagem Definida** **5.4.1** Observe os processos implementados e examine os mecanismos para verificar se os controles estão em vigor para detectar e proteger o pessoal contra ataques de phishing.	**Objetivo** Os controles técnicos podem limitar o número de ocasiões em que os funcionários precisam avaliar a veracidade de uma comunicação e também podem limitar os efeitos das respostas individuais ao phishing. **Práticas Recomendadas** Ao desenvolver controles antiphishing, as entidades são incentivadas a considerar uma combinação de abordagens. Por exemplo, o uso de controles antispoofing, como Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), e Domain Keys Identified Mail (DKIM) ajudará a impedir que phishers falsifiquem o domínio da entidade e se façam passar por funcionários . A implantação de tecnologias para bloquear e-mails de phishing e malware antes que eles cheguem aos funcionários, como depuradores de links e antimalware do lado do servidor, pode reduzir incidentes e diminuir o tempo necessário para que os funcionários verifiquem e relatem ataques de phishing. Além disso, o treinamento de pessoal para reconhecer e relatar e-mails de phishing pode permitir que e-mails semelhantes sejam identificados e removidos antes de serem abertos. É recomendado (mas não obrigatório) que os controles antiphishing sejam aplicados em toda a organização de uma entidade. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		Definições Phishing é uma forma de engenharia social e descreve os diferentes métodos usados por invasores para induzir a equipe a divulgar informações confidenciais, como nomes e senhas de contas de usuários e dados da conta. Os invasores normalmente se disfarçam e tentam parecer uma fonte genuína ou confiável, orientando a equipe a enviar uma resposta por e-mail, clicar em um link da web ou inserir dados em um site comprometido. Mecanismos que podem detectar e prevenir tentativas de phishing são frequentemente incluídos em soluções antimalware. **Informações Adicionais** Consulte o seguinte para obter mais informações sobre phishing: *National Cyber Security Centre - Phishing Attacks: Defending your Organization*. *US Cybersecurity & Infrastructure Security Agency - Report Phishing Sites.*

Requisito 6: Desenvolver e Manter Sistemas e Software Seguros

Seções	
6.1	Os processos e mecanismos para desenvolver e manter sistemas e softwares seguros são definidos e compreendidos.
6.2	O software sob medida e personalizado são desenvolvidos com segurança.
6.3	Vulnerabilidades de segurança são identificadas e tratadas.
6.4	Os aplicativos web voltados para o público são protegidos contra ataques.
6.5	Mudanças em todos os componentes de sistema são administradas com segurança.

Visão Geral

Pessoas com más intenções podem usar vulnerabilidades de segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são corrigidas por patches de segurança fornecidos pelo fornecedor, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os componentes de sistema devem ter todos os patches de software apropriados para proteção contra a exploração e o comprometimento dos dados da conta por indivíduos mal-intencionados e softwares mal-intencionados.

Os patches de software apropriados são aqueles que foram avaliados e testados o suficiente para determinar se os patches não entram em conflito com as configurações de segurança existentes. Para software sob medida e personalizado, inúmeras vulnerabilidades podem ser evitadas aplicando processos de ciclo de vida de software (SLC) e técnicas de codificação seguras.

Os repositórios de código que armazenam o código do aplicativo, configurações de sistema ou outros dados de configuração que podem afetar a segurança dos dados da conta ou o CDE estão no escopo das avaliações do PCI DSS.

Consulte Relação entre o PCI DSS e os Padrões de Software do PCI SSC na página 7 para obter informações sobre o uso de software validado pelo PCI SSC e fornecedores de software e como o uso dos padrões de software do PCI SSC pode ajudar a cumprir os controles no Requisito 6.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

***Observação**: O Requisito 6 se aplica a todos os componentes de sistema, exceto para a seção 6.2 para desenvolvimento de software com segurança, que se aplica apenas a software sob medida e personalizado usado em qualquer componente de sistema incluído ou conectado ao CDE.*

Requisitos e Procedimentos de Teste		Diretriz
6.1 Os processos e mecanismos para desenvolver e manter sistemas e softwares seguros são definidos e compreendidos.		
Requisitos da Abordagem Definida **6.1.1** Todas as políticas e processos operacionais identificados no Requisito 6 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas.	**Procedimentos de Teste da Abordagem Definida** **6.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 6 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 6.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 6. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 6, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.
Objetivo da Abordagem Personalizada As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 6 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, os sistemas não serão mantidos com segurança e seu nível de segurança será reduzido. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
6.1.2 As funções e responsabilidades para a execução de atividades no Requisito 6 são documentadas, atribuídas e compreendidas.	**6.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 6 estão documentadas e atribuídas.	
	6.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 6 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 6 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
6.2 O software sob medida e personalizado são desenvolvidos com segurança.		
Requisitos da Abordagem Definida **6.2.1** O software sob medida e personalizado são desenvolvidos com segurança, da seguinte forma: • Com base nos padrões da indústria e/ou práticas recomendadas para desenvolvimento seguro. • De acordo com o PCI DSS (por exemplo, autenticação segura e registro de auditoria). • Incorporando a consideração de questões de segurança da informação durante cada estágio do ciclo de vida de desenvolvimento de software. **Objetivo da Abordagem Personalizada** O software sob medida e personalizado é desenvolvido de acordo com o PCI DSS e processos de desenvolvimento seguros em todo o ciclo de vida do software. **Observações de Aplicabilidade** Isso se aplica a todos os softwares desenvolvidos para ou pela entidade para uso próprio da entidade. Isso inclui software sob medida e personalizado. Isso não se aplica a software de terceiros.	**Procedimentos de Teste da Abordagem Definida** **6.2.1** Examine os procedimentos de desenvolvimento de software documentados para verificar se os processos definidos incluem todos os elementos especificados neste requisito.	**Objetivo** Sem a inclusão da segurança durante as fases de definição de requisitos, design, análise e teste do desenvolvimento de software, as vulnerabilidades de segurança podem ser introduzidas inadvertidamente ou maliciosamente no ambiente de produção. **Práticas Recomendadas** Entender como os dados confidenciais são tratados pelo aplicativo - incluindo quando armazenados, transmitidos e na memória - pode ajudar a identificar onde os dados precisam ser protegidos. Os requisitos do PCI DSS devem ser considerados ao desenvolver software para atender a esses requisitos por design, em vez de tentar retroceder o software posteriormente. **Exemplos** Metodologias e estruturas de gerenciamento de ciclo de vida de software seguro incluem PCI Secure Software Framework, BSIMM, OPENSAMM e trabalhos do NIST, ISO e SAFECode.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
Ter uma equipe com conhecimento em métodos de codificação segura, incluindo técnicas definidas no Requisito 6.2.4, ajudará a minimizar o número de vulnerabilidades de segurança introduzidas por meio de práticas de codificação inadequadas.
Práticas Recomendadas
O treinamento para desenvolvedores pode ser fornecido internamente ou por terceiros.
O treinamento deve incluir, mas não está limitado a, linguagens de desenvolvimento em uso, design de software seguro, técnicas de codificação segura, uso de técnicas/métodos para encontrar vulnerabilidades no código, processos para prevenir a reintrodução de vulnerabilidades previamente resolvidas e como usar qualquer ferramenta de teste de segurança automatizado para detectar vulnerabilidades em software.
Conforme as práticas de codificação seguras aceitas pela indústria mudam, as práticas de codificação da organização e o treinamento do desenvolvedor podem precisar ser atualizados para lidar com novas ameaças.</td></tr>
<tr><td>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 segura.
• Incluindo, se ferramentas de teste de segurança são usadas, como usar as ferramentas para detectar vulnerabilidades no software.</td><td>6.2.2.a Examine os procedimentos de desenvolvimento de software para verificar se os processos são definidos para o treinamento do pessoal de desenvolvimento de software que desenvolve software sob medida e personalizado que inclui todos os elementos especificados neste requisito.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
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 à assistência e orientação quando necessário.</td><td>6.2.2.b Examine os registros de treinamento e entreviste o pessoal para verificar se o pessoal de desenvolvimento de software que trabalha com software sob medida e personalizado recebeu treinamento de segurança de software que seja relevante para sua função de trabalho e linguagens de desenvolvimento de acordo com todos os elementos especificados neste requisito.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
6.2.3 O software sob medida e personalizado 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 software existentes e emergentes. • As correções apropriadas são implementadas antes do lançamento.	**6.2.3.a** Examine os procedimentos de desenvolvimento de software documentados e entreviste o pessoal responsável para verificar se os processos definidos exigem que todo o software sob medida e personalizado seja revisado de acordo com todos os elementos especificados neste requisito.	Vulnerabilidades de segurança em software sob medida e personalizado são comumente exploradas por indivíduos mal-intencionados para obter acesso a uma rede e comprometer os dados da conta. O código vulnerável é muito mais difícil e caro de resolver depois de ter sido implantado ou lançado em ambientes de produção. Exigir uma revisão formal e aprovação da gerência antes do lançamento ajuda a garantir que o código seja aprovado e desenvolvido de acordo com as políticas e procedimentos.
Objetivo da Abordagem Personalizada	**6.2.3.b** Examine as evidências de mudanças no software sob medida e personalizado para verificar se as mudanças no código foram revisadas de acordo com todos os elementos especificados neste requisito.	**Práticas Recomendadas** Os seguintes itens devem ser considerados para inclusão nas revisões de código: • Procurando recursos não documentados (ferramentas de implante, backdoors). • Confirmando que o software usa com segurança as funções dos componentes externos (bibliotecas, estruturas, APIs, etc.). Por exemplo, se uma biblioteca de terceiros que fornece funções criptográficas for usada, verifique se ela foi integrada com segurança. • Verificando o uso correto do registro de auditoria para evitar que dados confidenciais entrem nos registros. • Análise de estruturas de código inseguras que podem conter vulnerabilidades potenciais relacionadas a ataques de software comuns identificados nos Requisitos 6.2.5. • Verificando o comportamento da aplicação para detectar vulnerabilidades lógicas.
O software sob medida e personalizado não pode ser explorado por meio de vulnerabilidades de codificação.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **6.2.3.1** Se as revisões manuais de código forem realizadas para software sob medida e personalizado 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 de codificação segura. • Revisados e aprovados pela gestão antes do lançamento. **Objetivo da Abordagem Personalizada** O processo de revisão manual de código não pode ser contornado e é eficaz na descoberta de vulnerabilidades de segurança. **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 ser gestor.	**Procedimentos de Teste da Abordagem Definida** **6.2.3.1.a** Se as revisões manuais de código forem realizadas para software sob medida e personalizado antes do lançamento para produção, examine os procedimentos de desenvolvimento de software documentados e entreviste o pessoal responsável para verificar se os processos são definidos para revisões manuais de código a serem conduzidas de acordo com todos os elementos especificados neste requisito. **6.2.3.1.b** Examine as evidências de mudanças no software sob medida e personalizado e entreviste o pessoal para verificar se as revisões manuais do código foram conduzidas de acordo com todos os elementos especificados neste requisito.	**Objetivo** Ter o código revisado por alguém que não seja o autor original, que tem experiência em revisões de código e conhecimento sobre práticas de codificação segura, minimiza a possibilidade de que o código contendo erros de segurança ou lógica que podem afetar a segurança dos dados do titular do cartão seja lançado em um ambiente de produção. Exigir a aprovação da gerência para que o código tenha sido revisado limita a capacidade do processo ser contornado. **Práticas Recomendadas** Descobriu-se que ter uma metodologia de revisão formal e listas de verificação de revisão melhora a qualidade do processo de revisão de código. A revisão do código é um processo cansativo e, por esse motivo, é mais eficaz quando os revisores revisam apenas pequenas quantidades de código por vez. Para manter a eficácia das revisões de código, é benéfico monitorar a carga de trabalho geral dos revisores e fazer com que revisem os aplicativos com os quais estão familiarizados. As revisões de código podem ser realizadas usando processos manuais ou automatizados ou uma combinação de ambos. Entidades que dependem exclusivamente da revisão manual do código devem garantir que os revisores mantenham suas habilidades por meio de treinamento regular conforme novas vulnerabilidades são encontradas e novos métodos de codificação seguros são recomendados. **Informações Adicionais** Consulte o *OWASP Code Review Guide.*

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
6.2.4 Técnicas de engenharia de software ou outros métodos são definidos e em uso pela equipe de desenvolvimento de software para prevenir ou mitigar ataques de software comuns e vulnerabilidades relacionadas para software sob medida e personalizado, incluindo, mas não se limitando ao seguinte: • Ataques de injeção, incluindo SQL, LDAP, XPath ou outro comando, parâmetro, objeto, falha ou falhas do tipo injeção. • 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. • 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 cross-site scripting (XSS) e cross-site request forgery (CSRF). *(continua na página a seguir)*	**6.2.4** Examine os procedimentos documentados e entreviste o pessoal responsável pelo desenvolvimento de software para verificar se as técnicas de engenharia de software ou outros métodos estão definidos e em uso por desenvolvedores de software sob medida e personalizado para prevenir ou mitigar todos os ataques de software comuns, conforme especificado neste requisito.	**Objetivo** Detectar ou prevenir erros comuns que resultam em código vulnerável o mais cedo possível no processo de desenvolvimento de software diminui a probabilidade de que tais erros cheguem à produção e levem a um comprometimento. Ter técnicas e ferramentas formais de engenharia incorporadas ao processo de desenvolvimento detectará esses erros logo no início. Essa filosofia às vezes é chamada de "shifting security left [mudando a segurança para a esquerda]". **Práticas Recomendadas** Tanto para software sob medida quanto para software personalizado, a entidade deve garantir que o código seja desenvolvido com foco na prevenção ou mitigação de ataques de software comuns, incluindo: • Tentativas de explorar vulnerabilidades comuns de codificação (bugs). • Tentativas de explorar falhas de design de software. • Tentativas de explorar falhas de implementação/configuração. • Ataques de enumeração - ataques automatizados que são explorados ativamente em pagamentos e identificação de abuso, autenticação ou mecanismos de autorização. Consulte o artigo do blog *PCI Perspectives "Beware of Account Testing Attacks*." Pesquisar e documentar técnicas de engenharia de software ou outros métodos ajuda a definir como os desenvolvedores de software evitam ou mitigam vários ataques de software por recursos ou contramedidas que eles incorporam ao software. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
• 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 vulnerabilidades, conforme definido no Requisito 6.3.1.		Isso pode incluir mecanismos de identificação/autenticação, controle de acesso, rotinas de validação de entrada, etc. Os desenvolvedores devem estar familiarizados com os diferentes tipos de vulnerabilidades e ataques potenciais e usar medidas para evitar vetores de ataque potenciais ao desenvolver o código. **Exemplos** As técnicas incluem processos automatizados e práticas que verificam o código no início do ciclo de desenvolvimento, quando o código é verificado para confirmar que as vulnerabilidades não estão presentes.
Objetivo da Abordagem Personalizada O software sob medida e personalizado não pode ser explorado por meio de ataques comuns e vulnerabilidades relacionadas.		
Observações de Aplicabilidade Isso se aplica a todos os softwares desenvolvidos para ou pela entidade para uso próprio da entidade. Isso inclui software sob medida e personalizado. Isso não se aplica a software de terceiros.		

Requisitos e Procedimentos de Teste		Diretriz
6.3 Vulnerabilidades de segurança são identificadas e tratadas.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
6.3.1 As vulnerabilidades de segurança são identificadas e gerenciadas da seguinte forma: • Novas vulnerabilidades de segurança são identificadas usando fontes reconhecidas pela indústria 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 da indústria 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.	**6.3.1.a** Examine as políticas e procedimentos para identificar e gerenciar vulnerabilidades de segurança para verificar se os processos estão definidos de acordo com todos os elementos especificados neste requisito. **6.3.1.b** Entreviste a equipe responsável, examine a documentação e observe os processos para verificar se as vulnerabilidades de segurança são identificadas e gerenciadas de acordo com todos os elementos especificados neste requisito.	**Objetivo** Classificar os riscos (por exemplo, como crítico, alto, médio ou baixo) permite que as organizações identifiquem, priorizem e tratem dos itens de maior risco mais rapidamente e reduzam a probabilidade de que as vulnerabilidades que representam o maior risco sejam exploradas. **Práticas Recomendadas** Os métodos para avaliar vulnerabilidades e atribuir classificações de risco variam com base no ambiente de uma organização e na estratégia de avaliação de risco. Quando uma entidade está atribuindo suas classificações de risco, ela deve considerar o uso de uma metodologia formal, objetiva e justificável que retrate com precisão os riscos das vulnerabilidades pertinentes à organização e se traduza em uma prioridade de resolução atribuída apropriadamente pela entidade. Os processos de uma organização para gerenciar vulnerabilidades devem ser integrados a outros processos de gerenciamento - por exemplo, gerenciamento de riscos, gerenciamento de

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada As vulnerabilidades de novos sistemas e softwares que podem afetar a segurança dos dados da conta ou do CDE são monitoradas, catalogadas e avaliadas quanto aos riscos.		mudanças, gerenciamento de patches, resposta a incidentes, segurança de aplicativos, bem como monitoramento adequado e registro desses processos. Isso ajudará a garantir que todas as vulnerabilidades sejam devidamente identificadas e tratadas. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Este requisito não é atendido nem é o mesmo que as varreduras de vulnerabilidade realizadas para os Requisitos 11.3.1 e 11.3.2. Esse requisito é para um processo monitorar ativamente as fontes de informações de vulnerabilidade da indústria e para a entidade determinar a classificação de risco a ser associada a cada vulnerabilidade.		Os processos devem apoiar a avaliação contínua de vulnerabilidades. Por exemplo, uma vulnerabilidade inicialmente identificada como de baixo risco pode se tornar um risco mais alto posteriormente. Além disso, as vulnerabilidades, individualmente consideradas de baixo ou médio risco podem representar coletivamente um risco alto ou crítico se estiverem presentes no mesmo sistema ou se exploradas em um sistema de baixo risco que possa resultar no acesso ao CDE. **Exemplos** Algumas organizações que emitem alertas para avisar as entidades sobre vulnerabilidades urgentes que requerem patches/atualizações imediatas são CERTs (Equipes de Resposta a Emergências de Computador) e fornecedores nacionais. Os critérios para classificação de vulnerabilidades podem incluir criticidade de uma vulnerabilidade identificada em um alerta do Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) ou um CERT, Common Vulnerability Scoring System (CVSS), a classificação pelo fornecedor e/ou tipo de sistemas afetados. **Informações Adicionais** Fontes confiáveis de informações de vulnerabilidade incluem sites de fornecedores, grupos de notícias da indústria, listas de mala direta, etc. Se o software for desenvolvido internamente, a equipe de desenvolvimento interna também deve considerar fontes de informação sobre novas vulnerabilidades que podem afetar os aplicativos desenvolvidos internamente. Outros métodos para garantir que novas vulnerabilidades sejam identificadas incluem soluções que reconhecem e alertam automaticamente ao detectar comportamentos incomuns. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		Os processos devem ser responsáveis por explorações amplamente publicadas, bem como ataques de “dia zero”, que visam vulnerabilidades anteriormente desconhecidas. Para software sob medida e personalizado, a organização pode obter informações sobre bibliotecas, estruturas, compiladores, linguagens de programação, etc. de fontes públicas confiáveis (por exemplo, recursos especiais e recursos de desenvolvedores de componentes). A organização também pode analisar independentemente componentes de terceiros e identificar vulnerabilidades. Para controle sobre o software desenvolvido internamente, a organização pode receber tais informações de fontes externas. A organização pode considerar o uso de um programa de “bug bounty [recompensa por bug]”, no qual posta informações (por exemplo, em seu site) para que terceiros possam contatar a organização com informações de vulnerabilidade. Fontes externas podem incluir investigadores independentes ou empresas que reportam à organização sobre vulnerabilidades identificadas e podem incluir fontes como o Common Vulnerability Scoring System (CVSS) ou a OWASP Risk Rating Methodology.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Vulnerabilidades conhecidas em componentes de software de terceiros não podem ser exploradas em software sob medida e personalizado. **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.*	**Procedimentos de Teste da Abordagem Definida** **6.3.2.a** Examine a documentação e entreviste a equipe para verificar se um inventário de software sob medida e personalizado e componentes de software de terceiros incorporados ao software sob medida e personalizado é mantido, e se o inventário é usado para identificar e resolver vulnerabilidades. **6.3.2.b** Examine a documentação do software, incluindo software sob medida e personalizado que integra componentes de software de terceiros, e compare-o com o inventário para verificar se o inventário inclui o software sob medida e personalizado e componentes de software de terceiros.	**Objetivo** Identificar e listar todos os softwares sob medida e personalizados da entidade e qualquer software de terceiros que seja incorporado ao software sob medida e personalizado da entidade permite que a entidade gerencie vulnerabilidades e patches. Vulnerabilidades em componentes de terceiros (incluindo bibliotecas, APIs, etc.) incorporados no software de uma entidade também tornam esses aplicativos vulneráveis a ataques. Saber quais componentes de terceiros são usados no software da entidade e monitorar a disponibilidade de patches de segurança para resolver vulnerabilidades conhecidas é fundamental para garantir a segurança do software. **Práticas Recomendadas** O inventário de uma entidade deve abranger todos os componentes e dependências de software de pagamento, incluindo plataformas ou ambientes de execução com suporte, bibliotecas de terceiros, serviços e outras funcionalidades necessárias. Existem muitos tipos diferentes de soluções que podem ajudar no gerenciamento de inventários de software, como ferramentas de análise de composição de software, ferramentas de descoberta de aplicativos e gerenciamento de dispositivos móveis.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
6.3.3 Todos os componentes de sistema são protegidos contra vulnerabilidades conhecidas, instalando patches/atualizações de segurança aplicáveis da seguinte forma: • Patches/atualizações críticos ou de alta segurança (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 entidade (por exemplo, dentro de três meses após o lançamento).	**6.3.3.a** Examine as políticas e procedimentos para verificar se os processos são definidos para abordar vulnerabilidades, instalando patches/atualizações de segurança aplicáveis de acordo com todos os elementos especificados neste requisito.	Novos “exploits” são constantemente descobertos e podem permitir ataques contra sistemas que antes eram considerados seguros. Se os patches/atualizações de segurança mais recentes não forem implementados em sistemas críticos assim que possível, um agente mal-intencionado pode usar esses “exploits” para atacar ou desabilitar um sistema ou obter acesso a dados confidenciais. **Práticas Recomendadas** A priorização de patches/atualizações de segurança para infraestrutura crítica garante que os sistemas e dispositivos de alta prioridade sejam protegidos contra vulnerabilidades o mais rápido possível após o lançamento de um patch. A cadência de patch de uma entidade deve levar em consideração qualquer reavaliação de vulnerabilidades e mudanças subsequentes na criticidade de uma vulnerabilidade de acordo com o Requisito 6.3.1. Por exemplo, uma vulnerabilidade inicialmente identificada como de baixo risco pode se tornar um risco mais alto posteriormente. Além disso, as vulnerabilidades individualmente consideradas de baixo ou médio risco podem representar coletivamente um risco alto ou crítico se estiverem presentes no mesmo sistema ou se exploradas em um sistema de baixo risco que possa resultar no acesso ao CDE.
Objetivo da Abordagem Personalizada	**6.3.3.b** Examine os componentes de sistema e o software relacionado e compare a lista de patches/atualizações de segurança instalados com as informações de patches/atualizações de segurança mais recentes para verificar se as vulnerabilidades são abordadas de acordo com todos os elementos especificados neste requisito.	
Os componentes de sistema não podem ser comprometidos pela exploração de uma vulnerabilidade conhecida.		

Requisitos e Procedimentos de Teste		Diretriz
6.4 Os aplicativos web voltados para o público são protegidos contra ataques.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Os aplicativos web voltados ao público são aqueles que estão disponíveis ao público (não apenas para uso interno). Esses aplicativos são os alvos principais dos invasores, e os aplicativos Web mal codificados fornecem um caminho fácil para os invasores obterem acesso a dados e sistemas confidenciais. **Práticas Recomendadas** As ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidade analisam e/ou testam o aplicativo em busca de vulnerabilidades. As ferramentas de avaliação comuns incluem scanners web especializados que realizam análises automáticas de proteção de aplicativos web. Ao usar soluções técnicas automatizadas, é importante incluir processos que facilitem respostas oportunas aos alertas gerados pelas soluções para que quaisquer ataques detectados possam ser mitigados. **Exemplos** Um firewall de aplicativo web (WAF) instalado na frente de aplicativos web voltados para o público para verificar todo o tráfego é um exemplo de uma solução técnica automatizada que detecta e evita ataques baseados na web (por exemplo, os ataques incluídos no Requisito 6.2.4). Os WAFs filtram e bloqueiam o tráfego não essencial na camada de aplicativo. Um WAF configurado corretamente ajuda a evitar ataques da camada de aplicativo em aplicativos que estão codificados ou configurados incorretamente. *(continua na página a seguir)*
6.4.1 Para aplicativos 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 web voltados para o público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de vulnerabilidade de segurança de aplicativos da seguinte maneira: – Pelo menos uma vez a cada 12 meses e após mudanças significativas. – Por uma entidade especializada em segurança de aplicações. – Incluindo, no mínimo, todos os ataques de software 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 soluções técnicas automatizadas que continuamente detectam e evitam ataques baseados na web da seguinte maneira: – Instalado na frente de aplicativos web voltados para o público para detectar e prevenir ataques baseados na web. – Executando ativamente e atualizado conforme aplicável.	**6.4.1** Para aplicativos web voltados para o público, certifique-se de que um dos métodos necessários esteja implementado da seguinte maneira: • Se ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidade estiverem em uso, examine os processos documentados, entreviste a equipe e examine os registros de avaliações de segurança de aplicativos para verificar se os aplicativos web voltados para o público são revisados de acordo com todos os elementos deste requisito específico para a ferramenta/método. **OU** • Se uma(s) solução(ões) técnica(s) automatizada(s) que continuamente detecta e evita ataques baseados na web está(ão) instalada(s), examine as definições de configuração do sistema e registros de auditoria e entreviste o pessoal responsável para verificar se a(s) solução(ões) técnica(s) automatizada(s) está(ão) instalada(s) de acordo com todos os elementos deste requisito específico para a(s) solução(ões).	

Requisitos e Procedimentos de Teste		Diretriz
– Gerando registros de auditoria. – Configurado para bloquear ataques baseados na web ou gerar um alerta que é investigado imediatamente.		Outro exemplo de solução técnica automatizada são as tecnologias Runtime Application Self-Protection (RASP). Quando implementadas corretamente, as soluções RASP podem detectar e bloquear o comportamento anômalo do software durante a execução. Enquanto os WAFs normalmente monitoram o perímetro do aplicativo, as soluções RASP monitoram e bloqueiam o comportamento no aplicativo.
Objetivo da Abordagem Personalizada Os aplicativos web voltados para o público são protegidos contra ataques maliciosos.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Aplicativos web voltados para o público são os alvos principais dos invasores, e os aplicativos web mal codificados fornecem um caminho fácil para os invasores obterem acesso a dados e sistemas confidenciais. **Práticas Recomendadas** Ao usar soluções técnicas automatizadas, é importante incluir processos que facilitem respostas oportunas aos alertas gerados pelas soluções para que quaisquer ataques detectados possam ser mitigados. Essas soluções também podem ser usadas para automatizar a mitigação, como por exemplo, controles de limitação de taxa, que podem ser implementados para mitigar ataques de força bruta e ataques de enumeração. **Exemplos** Um firewall de aplicativo web (WAF), que pode ser local ou baseado em nuvem, instalado na frente de aplicativos web voltados para o público para verificar todo o tráfego, é um exemplo de uma solução técnica automatizada que detecta e evita ataques baseados na web (por exemplo, os ataques incluídos no Requisito 6.2.4). Os WAFs filtram e bloqueiam o tráfego não essencial na camada de aplicativo. Um WAF configurado corretamente ajuda a evitar ataques da camada de aplicativo em aplicativos que estão codificados ou configurados incorretamente.
6.4.2 Para aplicativos 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 web voltados para o público e está configurado para detectar e prevenir ataques baseados na web. • Executando ativamente e atualizado conforme aplicável. • Gerando registros de auditoria. • Configurado para bloquear ataques baseados na web ou gerar um alerta que é investigado imediatamente.	**6.4.2** Para aplicativos web voltados para o público, examine as definições de configuração do sistema e registros de auditoria e entreviste a equipe responsável para verificar se uma solução técnica automatizada que detecta e evita ataques baseados na web está implementada de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
Os aplicativos web voltados para o público são protegidos em tempo real contra ataques maliciosos.		
Observações de Aplicabilidade		
Este novo requisito substituirá o Requisito 6.4.1 assim que sua data efetiva 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. • Um método é implementado para garantir a integridade de cada script. • Um inventário de todos os scripts é mantido com a justificativa por escrito de porque cada um é necessário. **Objetivo da Abordagem Personalizada** Código não autorizado não pode estar presente na página de pagamento, pois é processado no navegador do consumidor.	**Procedimentos de Teste da Abordagem Definida** **6.4.3.a** Examine as políticas e procedimentos para verificar se os processos são definidos para gerenciar todos os scripts da página de pagamento que são carregados e executados no navegador do consumidor, de acordo com todos os elementos especificados neste requisito. **6.4.3.b** Entreviste a equipe responsável e examine os registros de inventário e as configurações do sistema para verificar se todos os scripts da página de pagamento que são carregados e executados no navegador do consumidor são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** Scripts carregados e executados na página de pagamento podem ter sua funcionalidade alterada sem o conhecimento da entidade e também podem ter a funcionalidade de carregar scripts externos adicionais (por exemplo, publicidade e rastreamento, sistemas de gerenciamento de tags). Esses scripts aparentemente inofensivos podem ser usados por invasores em potencial para carregar scripts maliciosos que podem ler e exfiltrar os dados do titular do cartão do navegador do consumidor. Garantir que a funcionalidade de todos esses scripts seja entendida como necessária para a operação da página de pagamento minimiza o número de scripts que podem ser adulterados. Garantir que os scripts foram explicitamente autorizados reduz a probabilidade de scripts desnecessários serem adicionados à página de pagamento sem a aprovação apropriada da gerência. O uso de técnicas para evitar adulteração do script minimizará a probabilidade do script ser modificado para realizar um comportamento não autorizado, como copiar os dados do titular do cartão na página de pagamento. **Práticas Recomendadas** Os scripts podem ser autorizados por processos manuais ou automatizados (por exemplo, fluxo de trabalho). Onde a página de pagamento será carregada em um inline frame (IFRAME), restringir o local de onde a página de pagamento pode ser carregada, usando a Política de Segurança de Conteúdo (CSP) da página pode ajudar a evitar que conteúdo não autorizado seja substituído pela página de pagamento.

Requisitos e Procedimentos de Teste		Diretriz
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 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.*		**Definições** "Necessário" para este requisito significa que a revisão da entidade de cada script justifica e confirma por que é necessário para a funcionalidade da página de pagamento aceitar uma transação de pagamento. **Exemplos** A integridade dos scripts pode ser imposta por vários mecanismos diferentes, incluindo, mas não se limitando a: • Integridade de sub-recursos (SRI), que permite ao navegador do consumidor validar que um script não foi adulterado. • Um CSP, que limita os locais de onde o navegador do consumidor pode carregar um script e para onde transmitir os dados da conta. • Scripts proprietários ou sistemas de gerenciamento de tags, que podem impedir a execução de scripts maliciosos.

Requisitos e Procedimentos de Teste		Diretriz
6.5 Mudanças em todos os componentes de sistema são administradas com segurança.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Os procedimentos de gerenciamento de mudanças devem ser aplicados a todas as mudanças - incluindo a adição, remoção ou modificação de qualquer componente de sistema - no ambiente de produção. É importante documentar o motivo de uma mudança e a descrição da mudança para que as partes relevantes entendam e concordem que a mudança é necessária. Da mesma forma, documentar os impactos da mudança permite que todas as partes afetadas planejem adequadamente quaisquer mudanças em processamento. **Práticas Recomendadas** A aprovação por partes autorizadas confirma que a mudança é legítima e que a mudança é sancionada pela organização. As mudanças devem ser aprovadas por indivíduos com autoridade e conhecimento apropriados para entender o impacto da mudança. Testes completos pela entidade confirmam que a segurança do ambiente não é reduzida com a implementação de uma mudança e que todos os controles de segurança existentes permanecem implementados ou são substituídos por controles de segurança iguais ou mais fortes após a mudança. O teste específico a ser executado irá variar de acordo com o tipo de mudança e os componentes de sistema afetados. *(continua na página a seguir)*
6.5.1 As mudanças em todos os componentes de sistema no ambiente de produção são feitas de acordo com procedimentos estabelecidos que incluem: • Motivo e descrição da mudança. • Documentação do impacto na segurança. • Aprovação da 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 personalizados, todas as atualizações são testadas para conformidade com o Requisito 6.2.4 antes de serem implantadas em produção. • Procedimentos para resolver falhas e retornar a um estado seguro.	**6.5.1.a** Examine os procedimentos de controle de mudanças documentados para verificar se os procedimentos são definidos para mudanças em todos os componentes de sistema no ambiente de produção para incluir todos os elementos especificados neste requisito. **6.5.1.b** Examine as mudanças recentes nos componentes de sistema e rastreie essas mudanças até a documentação de controle de mudanças relacionada. Para cada mudança examinada, verifique se a mudança foi implementada de acordo com todos os elementos especificados neste requisito.	

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Todas as mudanças são rastreadas, autorizadas e avaliadas quanto ao impacto e segurança, e as mudanças são gerenciadas para evitar efeitos indesejados na segurança dos componentes de sistema.		Para cada mudança, é importante ter procedimentos documentados que tratem de quaisquer falhas e forneçam instruções sobre como retornar a um estado seguro caso a mudança falhe ou afete adversamente a segurança de um aplicativo ou sistema. Esses procedimentos permitirão que o aplicativo ou sistema seja restaurado ao seu estado seguro anterior.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **6.5.2** Após a conclusão de uma mudança significativa, todos os requisitos aplicáveis do PCI DSS são confirmados para estarem implementados em todos os sistemas e redes novos ou alterados, e a documentação é atualizada conforme aplicável. **Objetivo da Abordagem Personalizada** Todos os componentes de sistema são verificados após uma mudança significativa para estarem em conformidade com os requisitos do PCI DSS aplicáveis.	**Procedimentos de Teste da Abordagem Definida** **6.5.2** Examine a documentação para mudanças significativas, entreviste a equipe e observe os sistemas/redes afetados para verificar se a entidade confirmou que os requisitos do PCI DSS aplicáveis estavam implementados em todos os sistemas e redes novos ou alterados e que a documentação foi atualizada conforme aplicável.	**Objetivo** Ter processos para analisar mudanças significativas ajuda a garantir que todos os controles apropriados do PCI DSS sejam aplicados a quaisquer sistemas ou redes adicionados ou alterados dentro do ambiente dentro do escopo, e que os requisitos do PCI DSS continuem a ser atendidos para proteger o ambiente. **Práticas Recomendadas** A incorporação dessa validação nos processos de gerenciamento de mudanças ajuda a garantir que os inventários de dispositivos e os padrões de configuração sejam mantidos atualizados e que os controles de segurança sejam aplicados quando necessário. **Exemplos** Os requisitos aplicáveis do PCI DSS que podem ser afetados incluem, mas não estão limitados a: • Os diagramas de rede e de fluxo de dados são atualizados para refletir as mudanças. • Os sistemas são configurados de acordo com os padrões de configuração, com todas as senhas padrão alteradas e serviços desnecessários desabilitados. • Os sistemas são protegidos com os controles necessários - por exemplo, monitoramento de integridade de arquivos (FIM), antimalware, patches e registros de auditoria. • Os dados de autenticação confidenciais não são armazenados e todo o armazenamento de dados da conta é documentado e incorporado à política e procedimentos de retenção de dados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Essas mudanças significativas também devem ser capturadas e refletidas na atividade de confirmação de escopo do PCI DSS anual da entidade de acordo com o Requisito 12.5.2.		• Novos sistemas são incluídos no processo de varredura de vulnerabilidade trimestral. • Os sistemas são verificados em busca de vulnerabilidades internas e externas após mudanças significativas de acordo com os Requisitos 11.3.1.3 e 11.3.2.1.
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Devido ao estado em constante mudança dos ambientes de pré-produção, eles geralmente são menos seguros do que o ambiente de produção. **Práticas Recomendadas** As organizações devem compreender claramente quais ambientes são ambientes de teste ou de desenvolvimento e como esses ambientes interagem no nível de redes e aplicativos. **Definições** Os ambientes de pré-produção incluem desenvolvimento, teste, teste de aceitação do usuário (UAT), etc. Mesmo onde a infraestrutura de produção é usada para facilitar o teste ou o desenvolvimento, os ambientes de produção ainda precisam ser separados (lógica ou fisicamente) da funcionalidade de pré-produção, de modo que as vulnerabilidades introduzidas como resultado das atividades de pré-produção não afetem negativamente os sistemas de produção.
6.5.3 Os ambientes de pré-produção são separados dos ambientes de produção e a separação é aplicada com controles de acesso.	**6.5.3.a** Examine as políticas e procedimentos para verificar se os processos estão definidos para separar o ambiente de pré-produção do ambiente de produção por meio de controles de acesso que impõem a separação.	
	6.5.3.b Examine a documentação da rede e as configurações dos controles de segurança da rede para verificar se o ambiente de pré-produção está separado do(s) ambiente(s) de produção.	
Objetivo da Abordagem Personalizada Os ambientes de pré-produção não podem introduzir riscos e vulnerabilidades nos ambientes de produção.	**6.5.3.c** Examine as configurações de controle de acesso para verificar se os controles de acesso estão implementados para impor a separação entre os ambientes de pré-produção e de produção.	

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**6.5.4.a** Examine as políticas e procedimentos para verificar se os processos são definidos para separar papeis e funções para fornecer responsabilidade de modo que apenas as mudanças revisadas e aprovadas sejam implantadas.	O objetivo de separar papeis e funções entre os ambientes de produção e pré-produção é reduzir o número de pessoal com acesso ao ambiente de produção e aos dados da conta e, assim, minimizar o risco de acesso não autorizado, não intencional ou inadequado aos dados e componentes de sistema e ajudar a garantir que esse acesso é limitado aos indivíduos com necessidade de negócio para tal acesso. A intenção desse controle é separar atividades críticas para fornecer supervisão e revisão para detectar erros e minimizar as chances de fraude ou roubo (já que duas pessoas precisariam entrar em conluio para ocultar uma atividade). A separação de papeis e funções, também conhecida como separação ou segregação de funções, é um conceito importante de controle interno para proteger os ativos de uma entidade.
Objetivo da Abordagem Personalizada	**6.5.4.b** Observe os processos e entreviste o pessoal para verificar se os controles implementados separam os papeis e funções e fornecem responsabilidade de modo que apenas as mudanças revisadas e aprovadas sejam implementadas.	
As funções de trabalho e responsabilidades que diferenciam as atividades de pré-produção e produção são definidas e gerenciadas para minimizar o risco de ações não autorizadas, não intencionais ou inadequadas.		
Observações de Aplicabilidade		
Em ambientes com pessoal limitado, onde os indivíduos desempenham vários papeis ou funções, esse mesmo objetivo pode ser alcançado com controles procedimentais 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
6.5.5 Os PANs ativos 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.	**6.5.5.a** Examine as políticas e procedimentos para verificar se os processos estão definidos para não usar PANs ativos em ambientes de pré-produção, exceto onde esses ambientes estão em um CDE e protegidos de acordo com todos os requisitos do PCI DSS aplicáveis.	**Objetivo** O uso de PANs ativos fora de CDEs protegidos oferece a indivíduos mal-intencionados a oportunidade de obter acesso não autorizado aos dados do titular do cartão. **Práticas Recomendadas** As entidades podem minimizar o armazenamento de PANs ativos armazenando-os apenas na pré-produção quando estritamente necessário para um propósito de teste específico e definido e excluindo com segurança esses dados após o uso. Se uma entidade exigir PANs projetados especificamente para fins de teste, eles podem ser obtidos com os adquirentes. **Definições** Os PANs ativos referem-se a PANs válidos (não PANs de teste) que podem ser usados para realizar transações de pagamento. Além disso, quando os cartões de pagamento expiram, o mesmo PAN costuma ser reutilizado com uma data de validade diferente. Todos os PANs devem ser verificados como incapazes de realizar transações de pagamento antes de serem excluídos do escopo do PCI DSS. É responsabilidade da entidade confirmar se os PANs não estão ativos.
	6.5.5.b Observe os processos de teste e entreviste a equipe para verificar se os procedimentos estão implementados para garantir que os PANs ativos não sejam usados em ambientes de pré-produção, exceto onde esses ambientes estão em um CDE e protegidos de acordo com todos os requisitos aplicáveis do PCI DSS.	
Objetivo da Abordagem Personalizada	**6.5.5.c** Examine os dados de teste de pré-produção para verificar se os PANs ativos não são usados em ambientes de pré-produção, exceto quando esses ambientes estiverem em um CDE e protegidos de acordo com todos os requisitos aplicáveis do PCI DSS.	
Os PANs ativos não podem estar presentes em ambientes de pré-produção fora do CDE.		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Esses dados podem fornecer informações sobre o funcionamento de um aplicativo ou sistema e são um alvo fácil para indivíduos não autorizados explorarem para obter acesso aos sistemas. A posse de tais informações pode facilitar o comprometimento do sistema e dos dados da conta relacionados.</td></tr>
<tr><td rowspan="2">6.5.6 Os dados e as contas de teste são removidos dos componentes de sistema antes que o sistema entre em produção.</td><td>6.5.6.a Examine as políticas e procedimentos para verificar se os processos estão definidos para a remoção de dados de teste e contas de teste dos componentes de sistema antes que o sistema entre em produção.</td></tr>
<tr><td>6.5.6.b Observe os processos de teste para software de prateleira e aplicativos internos e entreviste a equipe para verificar se os dados de teste e as contas de teste são removidos antes que um sistema entre em produção.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada

Dados de teste e contas de teste não podem existir em ambientes de produção.</td><td>6.5.6.c Examine os dados e contas de softwares recentemente instalados ou softwares comerciais atualizados e aplicativos internos para verificar se não há dados de teste ou contas de teste em sistemas em produção.</td></tr>
</table>

Implementar Medidas Fortes de Controle de Acesso

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

Seções	
7.1	Processos e mecanismos para restringir o acesso aos componentes de sistema e dados do titular do cartão por necessidade de negócios são definidos e compreendidos.
7.2	O acesso aos componentes de sistema e dados é definido e atribuído apropriadamente.
7.3	O acesso aos componentes de sistema e dados é gerenciado por meio de um(s) sistema(s) de controle de acesso.

Visão Geral

Indivíduos não autorizados podem obter acesso a dados ou sistemas críticos devido a regras e definições de controle de acesso ineficazes. Para garantir que os dados críticos só possam ser acessados por pessoal autorizado, sistemas e processos devem estar implementados para limitar o acesso com base na necessidade de conhecimento e de acordo com as responsabilidades do trabalho.

“Acesso” ou “direitos de acesso” são criados por regras que fornecem aos usuários acesso a sistemas, aplicativos e dados, enquanto “privilégios” permitem que um usuário execute uma ação ou função específica em relação a esse sistema, aplicativo ou dados. Por exemplo, um usuário pode ter direitos de acesso a dados específicos, mas se ele pode apenas ler esses dados, ou também pode alterar ou excluir os dados, é determinado pelos privilégios atribuídos do usuário.

“Necessidade de conhecimento” refere-se a fornecer acesso a apenas a menor quantidade de dados necessários para realizar um trabalho.

“Privilégios mínimos” refere-se a fornecer apenas o nível mínimo de privilégios necessários para realizar um trabalho.

Esses requisitos se aplicam a contas de usuário e acesso para funcionários, contratados, consultores e fornecedores internos e externos e outros terceiros (por exemplo, para fornecer suporte ou serviços de manutenção). Certos requisitos também se aplicam a contas de aplicativo e sistema usadas pela entidade (também chamadas de “contas de serviço”).

Esses requisitos não se aplicam aos consumidores (titulares de cartão).

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
7.1 Processos e mecanismos para restringir o acesso aos componentes de sistema e dados do titular do cartão por necessidade de negócios são definidos e compreendidos.		
Requisitos da Abordagem Definida **7.1.1** Todas as políticas e processos operacionais identificados no Requisito 7 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 7 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **7.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 7 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 7.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 7. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 7, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem designadas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
7.1.2 As funções e responsabilidades para a execução de atividades no Requisito 7 são documentadas, atribuídas e compreendidas.	**7.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 7 estão documentadas e atribuídas.	
	7.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 7 para verificar se as funções e responsabilidades são atribuídas conforme são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 7 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
7.2 O acesso aos componentes de sistema e dados é definido e atribuído apropriadamente.		
Requisitos da Abordagem Definida **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 de sistema e recursos de dados que se baseiam na classificação e funções do trabalho dos usuários. • Os privilégios mínimos necessários (por exemplo, usuário, administrador) para executar uma função de trabalho. **Objetivo da Abordagem Personalizada** Os requisitos de acesso são estabelecidos de acordo com as funções de trabalho, seguindo os princípios de privilégio mínimo e necessidade de conhecimento.	**Procedimentos de Teste da Abordagem Definida** **7.2.1.a** Examine as políticas e procedimentos documentados e entreviste o pessoal para verificar se o modelo de controle de acesso está definido de acordo com todos os elementos especificados neste requisito. **7.2.1.b** Examine as configurações do modelo de controle de acesso e verifique se as necessidades de acesso estão adequadamente definidas de acordo com todos os elementos especificados neste requisito.	**Objetivo** Definir um modelo de controle de acesso que seja apropriado para a tecnologia da entidade e filosofia de controle de acesso apoia uma forma consistente e uniforme de alocação de acesso e reduz a possibilidade de erros, como a concessão de direitos excessivos. **Práticas Recomendadas** Um fator a ser considerado ao definir as necessidades de acesso é o princípio da separação de funções. Este princípio tem o intuito de prevenir fraudes e uso indevido ou roubo de recursos. Por exemplo, 1) dividir funções de missão crítica e funções de suporte do sistema de informação entre diferentes indivíduos e/ou funções, 2) estabelecer funções de modo que as atividades de suporte do sistema de informação sejam realizadas por diferentes funções/indivíduos (por exemplo, gerenciamento de sistema, programação, configuração gerenciamento, garantia e teste de qualidade, e segurança de rede) e 3) garantia de que o pessoal de segurança que administra as funções de controle de acesso não administre também as funções de auditoria. Em ambientes onde um indivíduo executa várias funções, como operações de administração e segurança, as tarefas podem ser atribuídas de forma que nenhum indivíduo tenha controle de ponta a ponta de um processo sem um ponto de verificação independente. Por exemplo, a responsabilidade pela configuração e a responsabilidade pela aprovação de mudanças podem ser atribuídas a indivíduos separados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		Definições Os principais elementos de um modelo de controle de acesso incluem: • Recursos a serem protegidos (os sistemas/dispositivos/dados aos quais o acesso é necessário), • Funções de trabalho que precisam de acesso ao recurso (por exemplo, administrador do sistema, pessoal do call center, balconista) e • Quais atividades cada função de trabalho precisa realizar (por exemplo, leitura/gravação ou consulta). Uma vez que as funções de trabalho, recursos e atividades por funções de trabalho são definidas, os indivíduos podem ter acesso concedido. **Exemplos** Os modelos de controle de acesso que as entidades podem considerar incluem controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributo (ABAC). O modelo de controle de acesso usado por uma determinada entidade depende de seus negócios e necessidades de acesso.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A atribuição de privilégios mínimos ajuda a evitar que usuários sem conhecimento suficiente sobre o aplicativo alterem incorretamente ou acidentalmente a configuração do aplicativo ou alterem suas configurações de segurança. Impor privilégio mínimo também ajuda a minimizar o escopo do dano se uma pessoa não autorizada obtiver acesso a uma ID de usuário. **Práticas Recomendadas** Os direitos de acesso são concedidos a um usuário por atribuição a uma ou várias funções. A avaliação é atribuída de acordo com as funções específicas do usuário e com o escopo mínimo necessário para o trabalho. Ao atribuir acesso privilegiado, é importante atribuir aos indivíduos apenas os privilégios de que precisam para realizar seu trabalho (os "privilégios mínimos"). Por exemplo, o administrador de banco de dados ou administrador de backup não deve receber os mesmos privilégios que o administrador geral de sistemas. Depois que as necessidades são definidas para as funções do usuário (de acordo com o requisito 7.2.1 do PCI DSS), é fácil conceder acesso aos indivíduos de acordo com sua classificação e função de trabalho usando as funções já criadas. As entidades podem desejar considerar o uso de Administração de Acesso Privilegiado (PAM por sua acrônimo em inglês), que é um método para conceder acesso a contas privilegiadas apenas quando esses privilégios são necessários, revogando imediatamente esse acesso quando eles não forem mais necessários.
7.2.2 O acesso é atribuído a usuários, incluindo usuários privilegiados, com base em: • Classificação e função do trabalho. • Privilégios mínimos necessários para desempenhar as responsabilidades do trabalho.	**7.2.2.a** Examine as políticas e procedimentos para verificar se eles cobrem a atribuição de acesso aos usuários de acordo com todos os elementos especificados neste requisito.	
	7.2.2.b Examine as configurações de acesso do usuário, inclusive para usuários com privilégios, e entreviste a equipe de gerenciamento responsável para verificar se os privilégios atribuídos estão de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada O acesso a sistemas e dados é limitado apenas ao acesso necessário para executar funções de trabalho, conforme definido nas funções de acesso relacionadas.	**7.2.2.c** Entreviste a equipe responsável pela atribuição de acesso para verificar se o acesso de usuário privilegiado é atribuído de acordo com todos os elementos especificados neste requisito.	

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
A aprovação documentada (por exemplo, por escrito ou eletronicamente) garante que aqueles com acesso e privilégios sejam conhecidos e autorizados pela administração e que seu acesso seja necessário para a função de trabalho.</td></tr>
<tr><td>7.2.3 Os privilégios exigidos são aprovados por pessoal autorizado.</td><td>7.2.3.a Examine as políticas e procedimentos para verificar se eles definem os processos de aprovação de todos os privilégios por pessoal autorizado.</td></tr>
<tr><td rowspan="2">Objetivo da Abordagem Personalizada

Privilégios de acesso não podem ser concedidos a usuários sem autorização apropriada e documentada.</td><td>7.2.3.b Examine os IDs de usuário e os privilégios atribuídos e compare com as aprovações documentadas para verificar se:
• A aprovação documentada existe para os privilégios atribuídos.
• A aprovação foi por pessoal autorizado.
• Os privilégios especificados correspondem às funções atribuídas ao indivíduo.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 impróprio é endereçado. • A gerência reconhece que o acesso continua apropriado.	**7.2.4.a** Examine as políticas e procedimentos para verificar se eles definem os processos de revisão de todas as contas de usuário e privilégios de acesso relacionados, incluindo contas de terceiros/fornecedores, de acordo com todos os elementos especificados neste requisito.	A revisão regular dos direitos de acesso ajuda a detectar direitos de acesso excessivos remanescentes depois que as responsabilidades do trabalho do usuário mudam, as funções do sistema mudam ou outras modificações. Se direitos excessivos do usuário não forem revogados no devido tempo, eles podem ser usados por usuários mal-intencionados para acesso não autorizado. Essa revisão fornece outra oportunidade para garantir que as contas de todos os usuários desligados tenham sido removidas (se alguma delas tiver sido perdida no momento do desligamento), bem como para garantir que quaisquer terceiros que não precisam mais de acesso tenham seu acesso encerrado.
Objetivo da Abordagem Personalizada	**7.2.4.b** Entreviste a equipe responsável e examine os resultados documentados das análises periódicas das contas dos usuários para verificar se todos os resultados estão de acordo com todos os elementos especificados neste requisito.	**Práticas Recomendadas** Quando um usuário é transferido para uma nova função ou departamento, normalmente os privilégios e o acesso associados à função anterior não são mais necessários. O acesso contínuo a privilégios ou funções que não são mais necessários pode apresentar o risco de uso indevido ou erros. Portanto, quando as responsabilidades mudam, os processos que revalidam o acesso ajudam a garantir que o acesso do usuário seja apropriado para as novas responsabilidades do usuário. As entidades podem considerar a implementação de um processo regular e repetível para conduzir revisões de direitos de acesso e atribuir “proprietários de dados” que são responsáveis por gerenciar e monitorar o acesso aos dados relacionados à sua função de trabalho e que também garantem que o acesso do usuário permaneça atualizado e apropriado. *(continua na página a seguir)*
As atribuições de privilégios de conta são verificadas periodicamente pela gerência como corretas e as não conformidades são corrigidas.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Este requisito se aplica a todas as contas de usuário e aos privilégios de acesso relacionados, 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 para 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.*		Por exemplo, um gerente direto pode revisar o acesso da equipe mensalmente, enquanto o gerente sênior analisa o acesso de seus grupos trimestralmente, ambos fazendo atualizações de acesso conforme necessário. A intenção dessas práticas recomendadas é apoiar e facilitar a condução das revisões pelo menos uma vez a cada 6 meses.
Requisitos da Abordagem Definida **7.2.5** Todas as contas de aplicativo e de 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. **Objetivo da Abordagem Personalizada** Os direitos de acesso concedidos a contas de aplicativo e de sistema são limitados apenas ao acesso necessário para a operabilidade desse aplicativo ou sistema.	**Procedimentos de Teste da Abordagem Definida** **7.2.5.a** Examine as políticas e procedimentos para verificar se eles definem os processos para gerenciar e atribuir contas de aplicativo e sistema e privilégios de acesso relacionados de acordo com todos os elementos especificados neste requisito. **7.2.5.b** Examine os privilégios associados às contas do sistema e do aplicativo e entreviste a equipe responsável para verificar se as contas do aplicativo e do sistema e os privilégios de acesso relacionados são atribuídos e gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** É importante estabelecer o nível de acesso apropriado para contas de aplicativo ou de sistema. Se essas contas forem comprometidas, os usuários mal-intencionados receberão o mesmo nível de acesso concedido ao aplicativo ou sistema. Portanto, é importante garantir que o acesso limitado seja concedido às contas do sistema e do aplicativo da mesma forma que às contas do usuário. **Práticas Recomendadas** As entidades podem querer considerar o estabelecimento de uma linha de base ao configurar essas contas de aplicativo e de sistema, incluindo o seguinte, conforme aplicável à organização: *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
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.*		• Certifique-se de que a conta não seja membro de um grupo privilegiado, como administradores de domínio, administradores locais ou root. • Restringindo em quais computadores a conta pode ser usada. • Restringindo o horário de uso. • Remover quaisquer configurações adicionais, como acesso VPN e acesso remoto.
Requisitos da Abordagem Definida **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 direcionada 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 impróprio é endereçado. • A gerência reconhece que o acesso continua apropriado.	**Procedimentos de Teste da Abordagem Definida** **7.2.5.1.a** Examine as políticas e procedimentos para verificar se eles definem os processos de revisão de todos os aplicativos e contas de sistema e privilégios de acesso relacionados de acordo com todos os elementos especificados neste requisito. **7.2.5.1.b** Examine a análise de risco direcionada da entidade para a frequência de revisões periódicas de aplicativos e contas de sistema e privilégios de acesso relacionados para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1. **7.2.5.1.c** Entreviste a equipe responsável e examine os resultados documentados das revisões periódicas das contas de sistema e do aplicativo e privilégios relacionados para verificar se as revisões ocorrem de acordo com todos os elementos especificados neste requisito.	**Objetivo** A revisão regular dos direitos de acesso ajuda a detectar direitos de acesso excessivos remanescentes depois que as funções do sistema mudam ou ocorrem outras modificações no aplicativo ou no sistema. Se direitos excessivos não forem removidos quando não forem mais necessários, eles podem ser usados por usuários mal-intencionados para acesso não autorizado.
Objetivo da Abordagem Personalizada As atribuições de privilégios de aplicativos e contas de sistema são verificadas periodicamente pela gerência como corretas e as não conformidades são corrigidas.		

Requisitos e Procedimentos de Teste		Diretriz
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.*		
Requisitos da Abordagem Definida **7.2.6** Todo o acesso do usuário a repositórios de consulta de dados do titular do cartão armazenados 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 de CHD armazenados.	**Procedimentos de Teste da Abordagem Definida** **7.2.6.a** Examine as políticas e procedimentos e entreviste a equipe para verificar se os processos são definidos para conceder acesso do usuário aos repositórios de consulta dos dados do titular do cartão armazenados, de acordo com todos os elementos especificados neste requisito. **7.2.6.b** Examine as definições de configuração para consultar repositórios de dados do titular do cartão armazenados para verificar se estão de acordo com todos os elementos especificados neste requisito.	**Objetivo** O uso indevido do acesso de consulta a repositórios de dados do titular do cartão tem sido uma causa regular de comprometimento de dados. Limitar esse acesso aos administradores reduz o risco de tal acesso ser abusado por usuários não autorizados. **Definições** "Métodos programáticos" significa conceder acesso por meio de procedimentos armazenados em banco de dados que permitem aos usuários executar ações controladas aos dados em uma tabela, em vez de acesso direto e não filtrado ao repositório de dados pelos usuários finais (exceto para o(s) administrador(es) responsável(is), que precisam de acesso direto ao banco de dados para suas funções administrativas). **Práticas Recomendadas** As ações típicas do usuário incluem mover, copiar e excluir dados. Considere também o escopo do privilégio necessário ao conceder acesso. Por exemplo, o acesso pode ser concedido a objetos específicos, como elementos de dados, arquivos, tabelas, índices, visualizações e rotinas armazenadas. A concessão de acesso aos repositórios de dados do titular do cartão deve seguir o mesmo processo de todos os outros acessos concedidos, o que significa que é baseado em funções, com apenas os privilégios atribuídos a cada usuário que são necessários para desempenhar suas funções de trabalho.
Objetivo da Abordagem Personalizada O acesso direto a consultas não filtradas (ad hoc) aos repositórios de dados do titular do cartão é proibido, a menos que seja realizado por um administrador autorizado.		
Observações de Aplicabilidade Este requisito se aplica aos controles de acesso do usuário aos repositórios de consulta dos dados do titular do cartão armazenados. Consulte os Requisitos 7.2.5 e 7.2.5.1 e 8.6.1 a 8.6.3 para obter os controles para aplicativos e contas de sistema.		

Requisitos e Procedimentos de Teste		Diretriz
7.3 O acesso aos componentes de sistema e dados é gerenciado por meio de um(s) sistema(s) de controle de acesso.		
Requisitos da Abordagem Definida **7.3.1** Um sistema de controle de acesso está implementado que restringe o acesso com base na necessidade de conhecimento de um usuário e cobre todos os componentes de sistema. **Objetivo da Abordagem Personalizada** Os direitos e privilégios de acesso são gerenciados por meio de mecanismos destinados a esse fim.	**Procedimentos de Teste da Abordagem Definida** **7.3.1** Examine a documentação do fornecedor e as configurações do sistema para verificar se o acesso é gerenciado para cada componente de sistema por meio de um sistema de controle de acesso que restringe o acesso com base na necessidade de conhecimento de um usuário e cobre todos os componentes de sistema.	**Objetivo** Sem um mecanismo para restringir o acesso com base na necessidade de conhecimento do usuário, um usuário pode, sem saber, receber acesso aos dados do titular do cartão. Os sistemas de controle de acesso automatizam o processo de restrição de acesso e atribuição de privilégios.
Requisitos da Abordagem Definida **7.3.2** O(s) sistema(s) de controle de acesso são configurados para fazer cumprir as permissões atribuídas a indivíduos, aplicativos e sistemas com base na classificação e função do trabalho. **Objetivo da Abordagem Personalizada** Direitos e privilégios de acesso de contas individuais para sistemas, aplicativos e dados são herdados apenas da associação ao grupo.	**Procedimentos de Teste da Abordagem Definida** **7.3.2** Examine a documentação do fornecedor e as configurações do sistema para verificar se o(s) sistema(s) de controle de acesso está(ão) configurado(s) para fazer cumprir as permissões atribuídas a indivíduos, aplicativos e sistemas com base na classificação e função do trabalho.	**Objetivo** Restringir o acesso privilegiado com um sistema de controle de acesso reduz a oportunidade de erros na atribuição de permissões a indivíduos, aplicativos e sistemas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Uma configuração padrão “negar tudo” garante que ninguém tenha acesso, a menos que uma regra seja estabelecida especificamente concedendo tal acesso. **Práticas Recomendadas** É importante verificar a configuração padrão dos sistemas de controle de acesso porque alguns são definidos por padrão para “permitir tudo”, permitindo assim o acesso a menos/até que uma regra seja escrita para negá-lo especificamente.
7.3.3 O(s) sistema(s) de controle de acesso é (são) configurado(s) para “negar tudo” por padrão.	**7.3.3** Examine a documentação do fornecedor e as configurações do sistema para verificar se o(s) sistema(s) de controle de acesso está(ão) definido(s) como “negar tudo” por padrão.	
Objetivo da Abordagem Personalizada		
Os direitos e privilégios de acesso são proibidos, a menos que expressamente permitidos.		

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

Seções	
8.1	Processos e mecanismos para identificar usuários e autenticar o acesso aos componentes de sistema são definidos e compreendidos.
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.
8.3	Uma autenticação forte para usuários e administradores é estabelecida e gerenciada.
8.4	A autenticação multifator (MFA) é implementada para proteger o acesso ao CDE.
8.5	Os sistemas de autenticação multifator (MFA) são configurados para evitar o uso indevido.
8.6	O uso de contas de aplicativo e sistema e fatores de autenticação associados é estritamente gerenciados.

Visão Geral

Dois princípios fundamentais de identificação e autenticação de usuários são: 1) estabelecer a identidade de um indivíduo ou processo em um sistema de computador e 2) provar ou verificar se o usuário associado à identidade é quem afirma ser.

A identificação de um indivíduo ou processo em um sistema de computador é conduzida associando uma identidade a uma pessoa ou processo por meio de um identificador, como um usuário, sistema ou ID de aplicativo. Esses IDs (também chamados de “contas”) estabelecem fundamentalmente a identidade de um indivíduo ou processo, atribuindo uma identificação única a cada pessoa ou processo para distinguir um usuário ou processo de outro. Quando cada usuário ou processo pode ser identificado de forma exclusiva, isso garante que haja responsabilidade pelas ações realizadas por essa identidade. Quando essa responsabilidade está implementada, as ações tomadas podem ser rastreadas para usuários e processos conhecidos e autorizados.

O elemento usado para provar ou verificar a identidade é conhecido como fator de autenticação. Os fatores de autenticação são 1) algo que você conhece, como uma senha ou frase secreta, 2) algo que você possui, como um dispositivo de token ou cartão inteligente, ou 3) algo que você é, como um elemento biométrico.

O ID e o fator de autenticação juntos são considerados credenciais de autenticação e são usados para obter acesso aos direitos e privilégios associados a um usuário, aplicativo, sistema ou contas de serviço.

(continua na página a seguir)

Esses requisitos de identidade e autenticação baseiam-se nos princípios de segurança e nas práticas recomendadas aceitos pela indústria para dar suporte ao ecossistema de pagamento. *A NIST Special Publication 800-63, Digital Identity Guidelines* fornece informações adicionais sobre estruturas aceitáveis para identidade digital e fatores de autenticação. É importante observar que as *diretrizes de identidade digital do NIST* se destinam às agências federais dos Estados Unidos e devem ser vistas em sua totalidade. Espera-se que muitos dos conceitos e abordagens definidos nestas diretrizes funcionem entre si e não como parâmetros autônomos.

***Observação**: Salvo indicação em contrário no requisito, esses requisitos se aplicam **a todas as contas em todos os componentes de sistema**, a menos que especificamente indicado em um requisito individual, incluindo, mas não se limitando a:*

- *Contas de ponto de venda*
- *Contas com recursos administrativos*
- *Contas de sistema e aplicativo*
- *Todas as contas usadas para visualizar ou acessar os dados do titular do cartão ou para acessar sistemas com os dados do titular do cartão.*

Isso inclui contas usadas por funcionários, contratados, consultores, fornecedores internos e externos e outros terceiros (por exemplo, para fornecer suporte ou serviços de manutenção).

Certos requisitos não se aplicam a contas de usuário 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). Quando os itens não se aplicam, eles são anotados diretamente no requisito específico.

Esses requisitos não se aplicam a contas usadas por consumidores (titulares de cartão).

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
8.1 Processos e mecanismos para identificar usuários e autenticar o acesso aos componentes de sistema são definidos e compreendidos.		
Requisitos da Abordagem Definida **8.1.1** Todas as políticas e processos operacionais identificados no Requisito 8 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 8 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **8.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 8 são gerenciados de acordo com todos os elementos que são especificados neste requisito.	**Objetivo** O Requisito 8.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 8. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 8, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
8.1.2 As funções e responsabilidades para a execução de atividades no Requisito 8 são documentadas, atribuídas e compreendidas.	**8.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 8 estão documentadas e atribuídas.	
	8.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 8 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 8 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
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.		
Requisitos da Abordagem Definida **8.2.1** Todos os usuários recebem um ID exclusivo antes de permitir o acesso aos componentes de sistema ou aos dados do titular do cartão. **Objetivo da Abordagem Personalizada** Todas as ações de todos os usuários são atribuíveis a um indivíduo. **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 (como IDs usados por caixas em terminais de ponto de venda).	**Procedimentos de Teste da Abordagem Definida** **8.2.1.a** Entreviste a equipe responsável para verificar se todos os usuários possuem uma ID exclusiva para acesso aos componentes de sistema e aos dados do titular do cartão. **8.2.1.b** Examine os registros de auditoria e outras evidências para verificar se o acesso aos componentes de sistema e aos dados do titular do cartão podem ser identificados de forma exclusiva e associados a indivíduos.	**Objetivo** A capacidade de rastrear ações executadas em um sistema de computador até um indivíduo estabelece responsabilidade e rastreabilidade e é fundamental para estabelecer controles de acesso eficazes. Ao garantir que cada usuário seja identificado de forma única, em vez de usar uma ID para vários funcionários, uma organização pode manter a responsabilidade individual por ações e um registro efetivo no registro de auditoria por funcionário. Além disso, isso ajudará na resolução de problemas e contenção quando ocorrer mau uso ou intenção maliciosa.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
8.2.2 Contas 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 conta é evitado, a menos que seja necessário em uma circunstância excepcional. • O uso é limitado ao tempo necessário para a circunstância excepcional. • A justificativa de negócio para uso é documentada. • O uso é explicitamente aprovado pela gerência. • 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.	**8.2.2.a** Examine as listas de contas de usuário nos componentes de sistema e a documentação aplicável para verificar se as credenciais de autenticação compartilhadas são usadas apenas quando necessário, com exceção, e são gerenciadas de acordo com todos os elementos especificados neste requisito. **8.2.2.b** Examine as políticas e procedimentos de autenticação para verificar se os processos são definidos para credenciais de autenticação compartilhadas, de forma que sejam usados apenas quando necessário, com exceção, e sejam gerenciados de acordo com todos os elementos especificados neste requisito. **8.2.2.c** Entreviste os administradores do sistema para verificar se as credenciais de autenticação compartilhadas são usadas apenas quando necessário, em uma base de exceção, e são gerenciadas de acordo com todos os elementos especificados neste requisito.	Contas de grupo, compartilhadas ou genéricas (ou padrão) são normalmente fornecidas com software ou sistemas operacionais - por exemplo, root ou com privilégios associados a uma função específica, como um administrador. Se vários usuários compartilharem as mesmas credenciais de autenticação (por exemplo, conta de usuário e senha), será impossível rastrear o acesso do sistema e as atividades a um indivíduo. Por sua vez, isso evita que uma entidade atribua responsabilidade por, ou tenha um registro efetivo das ações de um indivíduo, uma vez que uma determinada ação poderia ter sido realizada por qualquer pessoa no grupo com conhecimento do ID do usuário e fatores de autenticação associados. A capacidade de associar indivíduos às ações executadas com uma conta é essencial para fornecer responsabilidade individual e rastreabilidade em relação a quem executou uma ação, qual ação foi executada e quando essa ação ocorreu. **Práticas Recomendadas** Se contas compartilhadas forem usadas por qualquer motivo, fortes controles de gerenciamento precisam ser estabelecidos para manter a responsabilidade individual e a rastreabilidade. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
Todas as ações realizadas por usuários com IDs genéricos, de sistema ou compartilhados são atribuíveis a um indivíduo.		
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 (como IDs usados por caixas em terminais de ponto de venda).		

Requisitos e Procedimentos de Teste		Diretriz
		Exemplos Ferramentas e técnicas podem facilitar o gerenciamento e a segurança desses tipos de contas e confirmar a identidade individual do usuário antes que o acesso a uma conta seja concedido. As entidades podem considerar cofres de senha ou outros controles gerenciados pelo sistema, como o comando *sudo*. Um exemplo de circunstância excepcional é quando todos os outros métodos de autenticação falharam e uma conta compartilhada é necessária para uso de emergência ou acesso de administrador tipo “quebrar o vidro”.
Requisitos da Abordagem Definida **8.2.3** ***Requisito adicional apenas para prestadores de serviços:*** Os prestadores de serviços com acesso remoto às instalações do cliente usam fatores de autenticação exclusivos para cada instalação do cliente. **Objetivo da Abordagem Personalizada** A credencial de um prestador de serviços usada para um cliente não pode ser usada para qualquer outro cliente.	**Procedimentos de Teste da Abordagem Definida** **8.2.3** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as políticas e procedimentos de autenticação e entreviste a equipe para verificar se os prestadores de serviços com acesso remoto às instalações do cliente usam fatores de autenticação exclusivos para acesso remoto às instalações de cada cliente.	**Objetivo** Os prestadores de serviços com acesso remoto às instalações do cliente normalmente usam esse acesso para oferecer suporte a sistemas POS POI ou fornecer outros serviços remotos. Se um prestador de serviços usa os mesmos fatores de autenticação para acessar vários clientes, todos os clientes do prestador de serviços podem ser facilmente comprometidos se um invasor comprometer esse fator. Os criminosos sabem disso e visam deliberadamente os prestadores de serviços em busca de um fator de autenticação compartilhado que lhes dê acesso remoto a muitos comerciantes por meio desse único fator. **Exemplos** Tecnologias como mecanismos multifatores que fornecem uma credencial exclusiva para cada conexão (como uma senha de uso único) também podem atender ao objetivo desse requisito.

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. Este requisito não se aplica a prestadores de serviços que acessam seus próprios ambientes de serviços compartilhados, onde vários ambientes de clientes estão hospedados. Se os funcionários do prestador de serviços usarem fatores de autenticação compartilhados para acessar remotamente as instalações do cliente, esses fatores devem ser exclusivos por cliente e gerenciados de acordo com o Requisito 8.2.2.		
Requisitos da Abordagem Definida **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 aprovação apropriada. • Implementado apenas com os privilégios especificados na aprovação documentada. **Objetivo da Abordagem Personalizada** Os eventos de ciclo de vida para IDs de usuário e fatores de autenticação não podem ocorrer sem a autorização apropriada. **Observações de Aplicabilidade** Este requisito se aplica a todas as contas de usuário, incluindo funcionários, contratados, consultores, trabalhadores temporários e fornecedores terceirizados.	**Procedimentos de Teste da Abordagem Definida** **8.2.4** Examine as autorizações documentadas em várias fases do ciclo de vida da conta (adições, modificações e exclusões) e examine as configurações do sistema para verificar se a atividade foi gerenciada de acordo com todos os elementos especificados neste requisito.	**Objetivo** É imperativo que o ciclo de vida de um ID de usuário (adições, exclusões e modificações) seja controlado de forma que apenas contas autorizadas possam executar funções, ações sejam auditáveis e privilégios sejam limitados apenas ao que é necessário. Os invasores geralmente comprometem uma conta existente e, em seguida, escalam os privilégios dessa conta para realizar atos não autorizados ou podem criar novos IDs para continuar suas atividades em segundo plano. É essencial detectar e responder quando as contas do usuário são criadas ou alteradas fora do processo normal de mudança ou sem a autorização correspondente.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
Se um funcionário ou terceiro / fornecedor deixou a empresa e ainda tem acesso à rede por meio de sua conta de usuário, pode ocorrer acesso desnecessário ou malicioso aos dados do titular do cartão - tanto pelo ex-funcionário quanto por um usuário malicioso que explora a conta antiga e/ou não utilizada.</td></tr>
<tr><td rowspan="2">8.2.5 O acesso para usuários desligados é imediatamente revogado.</td><td>8.2.5.a Examine as fontes de informação dos usuários desligados e Examine as listas de acesso dos usuários atuais - tanto para acesso local quanto remoto - para verificar se os IDs dos usuários desligados foram desativados ou removidos das listas de acesso.</td></tr>
<tr><td>8.2.5.b Entreviste o pessoal responsável a fim de verificar se todos os fatores de autenticação física - como cartões inteligentes, tokens, etc. - foram devolvidos ou desativados para usuários desligados.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
As contas de usuários desligados não podem ser usadas.</td><td colspan="2"></td></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
Contas que não são usadas regularmente são frequentemente alvos de ataques, pois é menos provável que quaisquer alterações, como uma senha alterada, sejam notadas. Como tal, essas contas podem ser mais facilmente exploradas e usadas para acessar os dados do titular do cartão.
Práticas Recomendadas
Quando for razoavelmente previsto que uma conta não será usada por um longo período de tempo, como uma licença prolongada, a conta deve ser desativada assim que a licença começar, em vez de esperar 90 dias.</td></tr>
<tr><td>8.2.6 Contas de usuário inativas são removidas ou desabilitadas dentro de 90 dias de inatividade.</td><td>8.2.6 Examine as contas de usuário e as informações do último logon e entreviste a equipe para verificar se todas as contas de usuário inativas foram removidas ou desabilitadas dentro de 90 dias de inatividade.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
Contas de usuário inativas não podem ser usadas.</td><td colspan="2"></td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Permitir que terceiros tenham acesso 24 horas por dia, 7 dias por semana aos sistemas e redes de uma entidade, caso precisem fornecer suporte, aumenta as chances de acesso não autorizado. Esse acesso pode resultar em um usuário não autorizado no ambiente de terceiros ou um indivíduo mal-intencionado usando o ponto de entrada externo sempre disponível na rede de uma entidade. Quando terceiros precisam de acesso 24 horas por dia, 7 dias por semana, isso deve ser documentado, justificado, monitorado e vinculado a motivos de serviço específicos. **Práticas Recomendadas** Habilitar o acesso apenas para os períodos de tempo necessários e desabilitá-lo assim que não for mais necessário ajuda a evitar o uso indevido dessas conexões. Além disso, considere atribuir a terceiros uma data de início e término para seu acesso de acordo com seu contrato de serviço. O monitoramento do acesso de terceiros ajuda a garantir que terceiros acessem apenas os sistemas necessários e apenas durante os períodos de tempo aprovados. Qualquer atividade incomum usando contas de terceiros deve ser acompanhada e resolvida.
8.2.7 As contas usadas por terceiros para acessar, dar suporte ou manter os componentes de sistema por meio de acesso remoto são gerenciadas da seguinte forma: • Habilitada apenas durante o período de tempo necessário e desabilitada quando não estiver em uso. • O uso é monitorado para atividades inesperadas.	**8.2.7** Entreviste a equipe, examine a documentação de gerenciamento de contas e examine as evidências para verificar se as contas usadas por terceiros para acesso remoto são gerenciadas de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
O acesso remoto de terceiros não pode ser usado, exceto quando especificamente autorizado e o uso é supervisionado pela gerência.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Uma sessão de usuário não pode ser usada, exceto pelo usuário autorizado. **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 (como IDs usados por caixas em terminais de ponto de venda). Este requisito não tem como objetivo impedir que atividades legítimas sejam realizadas enquanto o console/PC estiver desacompanhado.	**Procedimentos de Teste da Abordagem Definida** **8.2.8** Examine as definições de configuração do sistema para verificar se os recursos de tempo limite ocioso do sistema/sessão para sessões de usuário foram definidos para 15 minutos ou menos.	**Objetivo** Quando os usuários saem de perto de uma máquina aberta com acesso a componentes de sistema ou dados do titular do cartão, existe o risco de que a máquina possa ser usada por outras pessoas na ausência do usuário, resultando em acesso não autorizado à conta e/ou uso indevido. **Práticas Recomendadas** A reautenticação pode ser aplicada no nível do sistema para proteger todas as sessões em execução na máquina ou no nível do aplicativo. As entidades também podem considerar o conjunto de controles em sucessão para restringir ainda mais o acesso de uma sessão desacompanhada com o passar do tempo. Por exemplo, o protetor de tela pode ser ativado após 15 minutos e fazer logoff do usuário após uma hora. Contudo, os controles de limite de tempo devem equilibrar o risco de acesso e exposição com o impacto para o usuário e a finalidade do acesso. Se um usuário precisa executar um programa desde um computador desacompanhado, o usuário pode fazer login no computador para iniciar o programa e, em seguida, "bloquear" o computador para que ninguém mais possa usar o login do usuário enquanto o computador estiver desacompanhado. **Exemplos** Uma maneira de atender a esse requisito é configurar um protetor de tela automatizado para iniciar sempre que o console ficar ocioso por 15 minutos e exigir que o usuário conectado insira sua senha para desbloquear a tela.

Requisitos e Procedimentos de Teste		Diretriz
8.3 Uma autenticação forte para usuários e administradores é estabelecida e gerenciada.		
Requisitos da Abordagem Definida **8.3.1** Todo o acesso do usuário aos componentes de 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. **Objetivo da Abordagem Personalizada** Uma conta não pode ser acessada, exceto com uma combinação de identidade do usuário e um fator 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 (como IDs usados por caixas em terminais de ponto de venda). 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.	**Procedimentos de Teste da Abordagem Definida** **8.3.1.a** Examine a documentação que descreve o(s) fator(es) de autenticação usado(s) para verificar se o acesso do usuário aos componentes de sistema é autenticado por meio de pelo menos um fator de autenticação especificado neste requisito. **8.3.1.b** Para cada tipo de fator de autenticação usado com cada tipo de componente de sistema, observe uma autenticação para verificar se a autenticação está funcionando de forma consistente com o(s) fator(es) de autenticação documentado(s).	**Objetivo** Quando usado além de IDs exclusivos, um fator de autenticação ajuda a proteger os IDs de usuário de serem comprometidos, uma vez que o invasor precisa ter o ID exclusivo e comprometer o(s) fator(es) de autenticação associado(s). **Práticas Recomendadas** Uma abordagem comum para um indivíduo mal-intencionado comprometer um sistema é explorar fatores de autenticação fracos ou inexistentes (por exemplo, senhas/frases secretas). Exigir fatores de autenticação fortes ajuda a proteger contra esse ataque. **Informações Adicionais** Consulte *fidoalliance.org* para obter mais informações sobre o uso de tokens, cartões inteligentes ou biometria como fatores de autenticação.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Os dispositivos de rede e aplicativos são conhecidos por transmitir fatores de autenticação legíveis e não criptografados (como senhas e frases secretas) pela rede e/ou armazenar esses valores sem criptografia. Como resultado, um indivíduo mal-intencionado pode facilmente interceptar essas informações durante a transmissão usando um “sniffer” ou acessar diretamente fatores de autenticação não criptografados nos arquivos onde estão armazenados e, em seguida, usar esses dados para obter acesso não autorizado.</td></tr>
<tr><td rowspan="2">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 de sistema.</td><td>8.3.2.a Examine a documentação do fornecedor e as definições de configuração do sistema para verificar se os fatores de autenticação são tornados ilegíveis com criptografia forte durante a transmissão e armazenamento.</td></tr>
<tr><td>8.3.2.b Examine os repositórios de fatores de autenticação para verificar se eles estão ilegíveis durante o armazenamento.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada</td><td rowspan="2">8.3.2.c Examine as transmissões de dados para verificar se os fatores de autenticação estão ilegíveis durante a transmissão.</td></tr>
<tr><td>Os fatores de autenticação em texto não criptografado não podem ser obtidos, derivados ou reutilizados da interceptação de comunicações ou de dados armazenados.</td><td></td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Indivíduos mal-intencionados usam técnicas de "engenharia social" para se passar por um usuário de um sistema - por exemplo, ligando para um help desk e agindo como um usuário legítimo - para ter um fator de autenticação alterado para que possam usar uma ID de usuário válida. Exigir a identificação positiva de um usuário reduz a probabilidade de sucesso desse tipo de ataque. **Práticas Recomendadas** As modificações nos fatores de autenticação para os quais a identidade do usuário deve ser verificada incluem, mas não se limitam a, redefinições de senha, provisionamento de novos tokens de hardware ou software, e geração de novas chaves. **Exemplos** Os métodos para verificar a identidade de um usuário incluem uma pergunta/resposta secreta, informações baseadas em conhecimento e ligar de volta para o usuário em um número de telefone conhecido e previamente estabelecido.
8.3.3 A identidade do usuário é verificada antes de modificar qualquer fator de autenticação.	**8.3.3** Examine os procedimentos para modificar os fatores de autenticação e observe a equipe de segurança para verificar se quando um usuário solicita uma modificação de um fator de autenticação, a identidade do usuário é verificada antes que o fator de autenticação seja modificado.	
Objetivo da Abordagem Personalizada		
Indivíduos não autorizados não podem obter acesso ao sistema falsificando a identidade de um usuário autorizado.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **8.3.4** Tentativas de autenticação inválidas são limitadas por: • Bloquear o ID do usuário após no máximo 10 tentativas. • Definir a duração do bloqueio para um mínimo de 30 minutos ou até que a identidade do usuário seja confirmada. **Objetivo da Abordagem Personalizada** Um fator de autenticação não pode ser adivinhado em um ataque online de força bruta. **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 (como IDs usados por caixas em terminais de ponto de venda).	**Procedimentos de Teste da Abordagem Definida** **8.3.4.a** Examine as definições de configuração do sistema para verificar se os parâmetros de autenticação estão definidos para exigir que as contas de usuário sejam bloqueadas após, no máximo, 10 tentativas de logon inválidas. **8.3.4.b** Examine as definições de configuração do sistema para verificar se os parâmetros de senha estão definidos para exigir que, uma vez que uma conta de usuário seja bloqueada, ela permaneça bloqueada por um mínimo de 30 minutos ou até que a identidade do usuário seja confirmada.	**Objetivo** Sem mecanismos de bloqueio de conta implementados, um invasor pode tentar continuamente adivinhar uma senha por meio de ferramentas manuais ou automatizadas (por exemplo, quebra de senha) até que o invasor tenha sucesso e obtenha acesso à conta de um usuário. Se uma conta for bloqueada devido a alguém tentar continuamente adivinhar uma senha, os controles para atrasar a reativação da conta bloqueada impedem que o indivíduo mal-intencionado adivinhe a senha, pois ele terá que parar por no mínimo 30 minutos até que a conta seja reativada . **Práticas Recomendadas** Antes de reativar uma conta bloqueada, a identidade do usuário deve ser confirmada. Por exemplo, o administrador ou a equipe de help desk podem validar se o proprietário real da conta está solicitando a reativação ou pode haver mecanismos de autoatendimento de redefinição de senha que o proprietário da conta usa para verificar sua identidade.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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. • Obrigada a ser trocada imediatamente após o primeiro uso.	**8.3.5** Examine os procedimentos para definir e redefinir senha/frases-senha (se usado como fatores de autenticação para atender ao Requisito 8.3.1) e observe o pessoal de segurança para verificar se as senhas/frases secretas são definidas e redefinidas de acordo com todos os elementos especificados neste requisito.	Se a mesma senha/frase secreta for usada para cada novo usuário, um usuário interno, ex-funcionário ou indivíduo mal-intencionado pode saber ou descobrir facilmente o valor e usá-lo para obter acesso às contas antes que o usuário autorizado tente usar a senha.
Objetivo da Abordagem Personalizada		
Uma senha/frase secreta inicial ou de redefinição atribuída a um usuário não pode ser usada por um usuário não autorizado.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**8.3.6** Examine as definições de configuração do sistema para verificar se os parâmetros de complexidade da senha/frase secreta do usuário estão definidos de acordo com todos os elementos especificados neste requisito.	Senhas/frases secretas fortes podem ser a primeira linha de defesa em uma rede, já que um indivíduo mal-intencionado geralmente tentará primeiro encontrar contas com senhas fracas, estáticas ou inexistentes. Se as senhas forem curtas ou fáceis de adivinhar, é relativamente fácil para um indivíduo mal-intencionado encontrar essas contas fracas e comprometer uma rede disfarçado de uma ID de usuário válida. **Práticas Recomendadas** A força da senha/frase secreta depende da complexidade, do comprimento e da aleatoriedade da senha/frase secreta. As senhas/frases secretas devem ser suficientemente complexas, portanto, não é prático para um invasor adivinhar ou descobrir seu valor. As entidades podem considerar o acréscimo de complexidade maior, exigindo o uso de caracteres especiais e caracteres maiúsculos e minúsculos, além dos padrões mínimos descritos por este requisito. A complexidade adicional aumenta o tempo necessário para ataques de força bruta off-line de senhas/frases secretas com hash. Outra opção para aumentar a resistência das senhas a ataques de adivinhação é comparar as senhas/frases secretas propostas a uma lista de senhas ruins e fazer com que os usuários forneçam novas senhas para quaisquer senhas encontradas na lista.
Objetivo da Abordagem Personalizada		
Uma senha/frase secreta adivinhada não pode ser verificada por um ataque de força bruta on-line ou off-line.		
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 (como IDs usados por caixas em terminais de ponto de venda). • 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **8.3.7** Indivíduos não têm permissão para enviar uma nova senha/frase secreta que seja igual a qualquer uma das últimas quatro senhas/frase secretas usadas. **Objetivo da Abordagem Personalizada** Uma senha usada anteriormente não pode ser usada para obter acesso a uma conta por pelo menos 12 meses. **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 (como IDs usados por caixas em terminais de ponto de venda).	**Procedimentos de Teste da Abordagem Definida** **8.3.7** Examine as definições de configuração do sistema para verificar se os parâmetros de senha estão definidos para exigir que as novas senhas/frases secretas não sejam iguais às quatro senhas/frases secretas usadas anteriormente.	**Objetivo** Se o histórico de senha não for mantido, a eficácia da alteração de senhas é reduzida, pois as senhas anteriores podem ser reutilizadas continuamente. Exigir que as senhas não possam ser reutilizadas por um período reduz a probabilidade de que as senhas que foram adivinhadas ou testadas por força bruta sejam reutilizadas no futuro. As senhas ou frases secretas podem ter sido alteradas anteriormente devido a suspeita de comprometimento ou porque a senha ou frase secreta excedeu seu período de uso efetivo, ambos os motivos pelos quais as senhas usadas anteriormente não devem ser reutilizadas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Comunicar as políticas e procedimentos de autenticação a todos os usuários ajuda eles a compreender e cumprir as políticas. **Práticas Recomendadas** A orientação sobre a seleção de senhas fortes pode incluir sugestões para ajudar o pessoal a selecionar senhas difíceis de adivinhar que não contenham palavras do dicionário ou informações sobre o usuário, como ID do usuário, nomes de membros da família, data de nascimento, etc. A orientação para proteger os fatores de autenticação pode incluir não anotar senhas ou não salvá-las em arquivos inseguros e estar alerta para indivíduos mal-intencionados que podem tentar explorar suas senhas (por exemplo, ligando para um funcionário e pedindo sua senha para que o chamador possa " solucionar um problema"). Como alternativa, as entidades podem implementar processos para confirmar que as senhas atendem à política de senhas, por exemplo, comparando as opções de senha a uma lista de senhas inaceitáveis e fazendo com que os usuários escolham uma nova senha para qualquer uma que corresponda a uma da lista. Instruir os usuários a alterar as senhas se houver uma chance de que a senha não seja mais segura pode impedir que usuários mal-intencionados usem uma senha legítima para obter acesso não autorizado.
8.3.8 As políticas e procedimentos de autenticação são documentados e comunicados a todos os usuários, incluindo: • Orientação sobre como selecionar 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 secretas se houver qualquer suspeita ou conhecimento de que a senhas/frases secretas foram comprometidas e como relatar o incidente.	**8.3.8.a** Examine os procedimentos e entreviste a equipe para verificar se as políticas e procedimentos de autenticação são distribuídos a todos os usuários.	
	8.3.8.b Revise as políticas e procedimentos de autenticação que são distribuídos aos usuários e verifique se eles incluem os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada	**8.3.8.c** Entreviste usuários para verificar se eles estão familiarizados com as políticas e procedimentos de autenticação.	
Os usuários estão bem informados sobre o uso correto dos fatores de autenticação e podem acessar assistência e orientação quando necessário.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**8.3.9** Se as senhas/frases secretas forem usadas como o único fator de autenticação para o acesso do usuário, inspecione as definições de configuração do sistema para verificar se as senhas/frases secretas são gerenciadas de acordo com UM dos elementos especificados neste requisito.	O acesso aos componentes de sistema dentro do escopo que não estão no CDE pode ser fornecido usando um único fator de autenticação, como uma senha/frase secreta, dispositivo de token ou cartão inteligente ou atributo biométrico. Onde senhas/frases secretas são empregadas como o único fator de autenticação para tal acesso, controles adicionais são necessários para proteger a integridade da senha/frase secreta. **Práticas Recomendadas** As senhas/frases secretas que são válidas por um longo tempo sem alteração fornecem aos indivíduos mal-intencionados mais tempo para quebrar a senha/frase secreta. A troca periódica de senhas oferece menos tempo para que um indivíduo mal-intencionado decifre uma senha/frase secreta e menos tempo para usar uma senha comprometida. Usar uma senha/frase secreta como o único fator de autenticação fornece um ponto único de falha, se comprometido. Portanto, nessas implementações, os controles são necessários para minimizar por quanto tempo a atividade maliciosa pode ocorrer por meio de uma senha/frase secreta comprometida. Analisar dinamicamente a postura de segurança de uma conta é outra opção que permite detecção e resposta mais rápidas para lidar com credenciais potencialmente comprometidas. Essa análise leva uma série de pontos de dados, que podem incluir integridade do dispositivo, localização, tempos de acesso e os recursos acessados para determinar em tempo real se uma conta pode receber acesso a um recurso solicitado. Dessa forma, o acesso pode ser negado e as contas bloqueadas se houver suspeita de que as credenciais de autenticação foram comprometidas. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
Uma senha/frase secreta comprometida não detectada não pode ser usada indefinidamente.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Este requisito se aplica aos componentes do sistema dentro do escopo que não estão no CDE porque esses componentes não estão sujeitos aos requisitos do MFA. 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 (como IDs usados por caixas em terminais de ponto de venda). Este requisito não se aplica a contas de clientes de prestadores de serviços, mas se aplica a contas para funcionários de prestadores de serviços.		**Informações Adicionais** Para obter informações sobre como usar a análise dinâmica para gerenciar o acesso do usuário aos recursos, consulte *NIST SP 800-207 Zero Trust Architecture.*
Requisitos da Abordagem Definida **8.3.10** ***Requisito adicional apenas para prestadores de serviços:*** Se as senhas/frases secretas forem usadas como o único fator de autenticação para o acesso do usuário do cliente aos dados do titular do cartão (ou seja, em qualquer implementação de autenticação de fator único), então a orientação é fornecida aos usuários do cliente, incluindo: • Orientação para os clientes alterarem suas senhas/frases secretas de usuário periodicamente. • Orientação sobre quando e em que circunstâncias as senhas/frases secretas têm que ser alteradas.	**Procedimentos de Teste da Abordagem Definida** **8.3.10** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Se as senhas/frases secretas forem usadas como o único fator de autenticação para o acesso do usuário do cliente aos dados do titular do cartão, examine a orientação fornecida aos usuários do cliente para verificar se a orientação inclui todos os elementos especificados neste requisito.	**Objetivo** Usar uma senha/frase secreta como o único fator de autenticação fornece um ponto único de falha, se comprometido. Portanto, nessas implementações, os controles são necessários para minimizar por quanto tempo a atividade maliciosa pode ocorrer por meio de uma senha/frase secreta comprometida. **Práticas Recomendadas** As senhas/frases secretas que são válidas por um longo tempo sem alteração fornecem aos indivíduos mal-intencionados mais tempo para quebrar a senha/frase. A troca periódica de senhas oferece menos tempo para que um indivíduo mal-intencionado quebre uma senha/frase secreta e menos tempo para usar uma senha comprometida.
Objetivo da Abordagem Personalizada As senhas/ frases secretas para clientes dos prestadores de serviços não podem ser usadas indefinidamente.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. Este requisito não se aplica a contas de usuários consumidores que acessam suas próprias informações de cartão de pagamento. Este requisito para prestadores de serviço será substituído pelo Requisito 8.3.10.1 quando o 8.3.10.1 entrar em vigor.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
8.3.10.1 ***Requisito adicional apenas para prestadores de serviços:*** Se as senhas/frases secretas forem usadas como o único fator de autenticação para o acesso do usuário do cliente (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.	**8.3.10.1** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Se as senhas/frases secretas forem usadas como o único fator de autenticação para o acesso do usuário cliente, inspecione as definições de configuração do sistema para verificar se as senhas/frases secretas são gerenciadas de acordo com UM dos elementos especificados neste requisito.	Usar uma senha/frase secreta como o único fator de autenticação fornece um ponto único de falha, se comprometido. Portanto, nessas implementações, os controles são necessários para minimizar por quanto tempo a atividade maliciosa pode ocorrer por meio de uma senha/frase secreta comprometida. **Práticas Recomendadas** As senhas/frases secretas que são válidas por um longo tempo sem alteração fornecem aos indivíduos mal-intencionados mais tempo para quebrar a senha/frase secreta. A troca periódica de senhas oferece menos tempo para que um indivíduo mal-intencionado decifre uma senha/frase secreta e menos tempo para usar uma senha comprometida. Analisar dinamicamente a postura de segurança de uma conta é outra opção que permite detecção e resposta mais rápidas para lidar com credenciais potencialmente comprometidas. Essa análise leva uma série de pontos de dados, que podem incluir integridade do dispositivo, localização, tempos de acesso e os recursos acessados para determinar em tempo real se uma conta pode receber acesso a um recurso solicitado. Dessa forma, o acesso pode ser negado e as contas bloqueadas se houver suspeita de que as credenciais da conta foram comprometidas. **Informações Adicionais** Para obter informações sobre como usar a análise dinâmica para gerenciar o acesso do usuário aos recursos, consulte *NIST SP 800-207 Zero Trust Architecture*.
Objetivo da Abordagem Personalizada		
As senhas/frases secretas para clientes dos prestadores de serviços não podem ser usadas indefinidamente.		
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. Este requisito não se aplica a contas de usuários consumidores que acessam suas próprias informações de cartão de pagamento. *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 que este requisito entre em vigor em 31 de março de 2025, os prestadores de serviços podem atender ao Requisito 8.3.10 ou 8.3.10.1.		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Se vários usuários puderem usar fatores de autenticação, como tokens, cartões inteligentes e certificados, pode ser impossível identificar o indivíduo usando o mecanismo de autenticação.
Práticas Recomendadas
Ter controles físicos e/ou lógicos (por exemplo, um PIN, dados biométricos ou uma senha) para autenticar exclusivamente o usuário da conta impedirá que usuários não autorizados obtenham acesso à conta do usuário por meio do uso de um fator de autenticação compartilhado.</td></tr>
<tr><td rowspan="2">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.</td><td>8.3.11.a Examine as políticas e procedimentos de autenticação para verificar se os procedimentos para usar fatores de autenticação, como tokens de segurança física, cartões inteligentes e certificados, estão definidos e incluem todos os elementos especificados neste requisito.</td></tr>
<tr><td>8.3.11.b Entreviste a equipe de segurança para verificar se os fatores de autenticação são atribuídos a um usuário individual e não compartilhados entre vários usuários.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada</td><td rowspan="2">8.3.11.c Examine os parâmetros de configuração do sistema e/ou observe os controles físicos, conforme aplicável, para verificar se os controles são implementados para garantir que apenas o usuário pretendido pode usar esse fator para obter acesso.</td></tr>
<tr><td>Um fator de autenticação não pode ser usado por ninguém além do usuário ao qual está atribuído.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
8.4 A autenticação multifator (MFA) é implementada para proteger o acesso ao CDE.		
Requisitos da Abordagem Definida **8.4.1** O MFA é implementado para todos os acessos não-console no CDE para o pessoal com acesso administrativo. **Objetivo da Abordagem Personalizada** O acesso administrativo ao CDE não pode ser obtido pelo uso de um único fator de autenticação. **Observações de Aplicabilidade** O requisito de MFA para acesso administrativo não-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. O MFA é considerado uma prática recomendada para acesso administrativo não-console aos componentes de sistema dentro do escopo que não fazem parte do CDE.	**Procedimentos de Teste da Abordagem Definida** **8.4.1.a** Examine as configurações de rede e/ou sistema para verificar se o MFA é necessário para todos os acessos não-console no CDE para pessoal com acesso administrativo. **8.4.1.b** Observe a equipe do administrador fazendo login no CDE e verifique se o MFA é necessário.	**Objetivo** A exigência de mais de um tipo de fator de autenticação reduz a probabilidade de um invasor obter acesso a um sistema se mascarando como um usuário legítimo, porque o invasor precisaria comprometer vários fatores de autenticação. Isso é especialmente verdadeiro em ambientes onde tradicionalmente o único fator de autenticação empregado era algo que o usuário conhece, como uma senha ou frase secreta. **Definições** Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifator.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **8.4.2** O MFA é implementado para todos os acessos ao CDE. **Objetivo da Abordagem Personalizada** O acesso ao CDE não pode ser obtido pelo uso de um único fator de autenticação. **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). 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 por meio de acesso administrativo não-console da rede da entidade ao CDE. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **8.4.2.a** Examine as configurações de rede e/ou sistema para verificar se o MFA está implementado para todos os acessos ao CDE. **8.4.2.b** Observe o pessoal que faz o login no CDE e examine as evidências para verificar se o MFA é necessário.	**Objetivo** A exigência de mais de um tipo de fator de autenticação reduz a probabilidade de um invasor obter acesso a um sistema se mascarando como um usuário legítimo, porque o invasor precisaria comprometer vários fatores de autenticação. Isso é especialmente verdadeiro em ambientes onde tradicionalmente o único fator de autenticação empregado era algo que o usuário conhece, como uma senha ou frase secreta. **Definições** Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifator.

Requisitos e Procedimentos de Teste		Diretriz
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 acesso com base na web a um aplicativo ou função. O MFA para acesso remoto 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A exigência de mais de um tipo de fator de autenticação reduz a probabilidade de um invasor obter acesso a um sistema se mascarando como um usuário legítimo, porque o invasor precisaria comprometer vários fatores de autenticação. Isso é especialmente verdadeiro em ambientes onde tradicionalmente o único fator de autenticação empregado era algo que o usuário conhece, como uma senha ou frase secreta. **Definições** A autenticação multifator (MFA) requer que um indivíduo apresente um mínimo de dois dos três fatores de autenticação especificados no Requisito 8.3.1 antes que o acesso seja concedido. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifator.
8.4.3 O MFA é implementado para todos os acessos remotos à rede originados de fora da rede da entidade que podem acessar ou impactar o CDE da seguinte forma: • Todo o acesso remoto por todo o pessoal, tanto usuários quanto administradores, originado de fora da rede da entidade. • Todo o acesso remoto por terceiros e fornecedores.	**8.4.3.a** Examine as configurações de rede e/ou sistema para acesso remoto a servidores e sistemas para verificar se o MFA é necessário de acordo com todos os elementos especificados neste requisito.	
	8.4.3.b Observe a equipe (por exemplo, usuários e administradores) conectando-se remotamente à rede e verifique se a autenticação multifator é necessária.	
Objetivo da Abordagem Personalizada O acesso remoto à rede da entidade não pode ser obtido usando um único fator de autenticação.		

(continua na página a seguir)

Requisitos e Procedimentos de Teste		Diretriz
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. 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 acesso com base na web a um aplicativo ou função.		

Requisitos e Procedimentos de Teste		Diretriz
8.5 Os sistemas de autenticação multifator (MFA) são configurados para evitar o uso indevido.		
Requisitos da Abordagem Definida **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 gerência 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. **Objetivo da Abordagem Personalizada** Os sistemas MFA são resistentes a ataques e controlam estritamente qualquer anulação administrativa. **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.*	**Procedimentos de Teste da Abordagem Definida** **8.5.1.a** Examine a documentação do sistema do fornecedor para verificar se o sistema MFA não é suscetível a ataques de repetição. **8.5.1.b** Examine as configurações do sistema para a implementação do MFA para verificar se está configurado de acordo com todos os elementos especificados neste requisito. **8.5.1.c** Entreviste o pessoal responsável e observe os processos para verificar se todas as solicitações para contornar o MFA são especificamente documentadas e autorizadas pela gerência de forma excepcional, por um período de tempo limitado. **8.5.1.d** Observe a equipe fazendo login nos componentes do sistema no CDE para verificar se o acesso é concedido somente depois que todos os fatores de autenticação são bem-sucedidos. **8.5.1.e** Observe o pessoal se conectando remotamente de fora da rede da entidade para verificar se o acesso é concedido somente após todos os fatores de autenticação serem bem-sucedidos.	**Objetivo** Sistemas MFA mal configurados podem ser contornados por invasores. Este requisito, portanto, trata da configuração de sistema(s) MFA que fornecem MFA para usuários que acessam os componentes de sistema no CDE. **Definições** Usar um tipo de fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifator. **Informações Adicionais** Para obter mais informações sobre os sistemas e recursos do MFA, consulte o seguinte: *PCI SSC's Information Supplement: Multi-Factor Authentication* Perguntas frequentes (FAQs) do PCI SSC sobre este tópico.

Requisitos e Procedimentos de Teste		Diretriz
8.6 O uso de contas de aplicativo e sistema e fatores de autenticação associados é estritamente gerenciados.		
Requisitos da Abordagem Definida **8.6.1** Se as contas usadas por sistemas ou aplicativos podem ser usadas para login interativo, elas são gerenciados 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 de negócios para uso interativo é documentada. • O uso interativo é explicitamente aprovado pela gerência. • 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. **Objetivo da Abordagem Personalizada** Quando usadas interativamente, todas as ações com contas designadas como contas de sistema ou aplicativo são autorizadas e atribuíveis a um indivíduo. **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.*	**Procedimentos de Teste da Abordagem Definida** **8.6.1** Examine as contas do aplicativo e do sistema que podem ser usadas interativamente e entreviste a equipe administrativa para verificar se as contas do aplicativo e do sistema são gerenciadas de acordo com todos os elementos especificados neste requisito.	**Objetivo** Como contas de usuário individuais, contas de sistema e de aplicativo exigem responsabilidade e gerenciamento rigoroso para garantir que sejam usadas apenas para a finalidade pretendida e não sejam usadas indevidamente Os invasores geralmente comprometem as contas do sistema ou do aplicativo para obter acesso aos dados do titular do cartão. **Práticas Recomendadas** Sempre que possível, configure contas de sistema e de aplicativo para impedir o login interativo para evitar que indivíduos não autorizados façam login e usem a conta com seus privilégios de sistema associados, e para limitar as máquinas e dispositivos nos quais a conta pode ser usada. **Definições** Contas de sistema ou aplicativo são aquelas contas que executam processos ou tarefas em um sistema de computador ou aplicativo e não são normalmente contas nas quais um indivíduo faz logon. Essas contas geralmente têm privilégios elevados que são necessários para executar tarefas ou funções especializadas. Login interativo é a capacidade de uma pessoa fazer login em uma conta do sistema ou aplicativo da mesma maneira que uma conta de usuário normal. Usar contas do sistema e do aplicativo dessa forma significa que não há responsabilidade e rastreabilidade das ações tomadas pelo usuário.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A proteção inadequada das senhas/frases secretas usadas por contas de aplicativo e sistema, especialmente se essas contas puderem ser usadas para login interativo, aumenta o risco e o sucesso do uso não autorizado dessas contas privilegiadas. **Práticas Recomendadas** Alterar esses valores devido à divulgação suspeita ou confirmada pode ser particularmente difícil de implementar. As ferramentas podem facilitar o gerenciamento e a segurança dos fatores de autenticação para contas de aplicativo e sistema. Por exemplo, considere cofres de senha ou outros controles gerenciados pelo sistema.
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/proprietários ou código-fonte sob medida e personalizado.	**8.6.2.a** Entreviste a equipe e examine os procedimentos de desenvolvimento do sistema para verificar se os processos são definidos para aplicativos e contas do sistema que podem ser usados para login interativo, especificando que as senhas/frases secretas não são codificadas em scripts, arquivos de configuração/proprietários ou código-fonte sob medida e personalizado.	
	8.6.2.b Examine scripts, arquivos de configuração/proprietários e código-fonte sob medida e personalizado para contas de aplicativo e sistema que podem ser usadas para login interativo, para verificar se as senhas/frases secretas dessas contas não estão presentes.	
Objetivo da Abordagem Personalizada		
As senhas/frases secretas usadas por contas de aplicativo e sistema não podem ser usadas por pessoal não autorizado.		
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.*		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
As contas de sistemas e aplicativos representam mais risco de segurança inerente do que contas de usuário porque muitas vezes são executadas em um contexto de segurança elevado, com acesso a sistemas que podem não ser normalmente concedidos a contas de usuário, como acesso programático a bancos de dados etc. Como resultado, uma consideração especial deve ser dada à proteção de senhas/frases secretas usadas para contas e aplicativos do sistema.
Práticas Recomendadas
As entidades devem considerar os seguintes fatores de risco ao determinar como proteger as senhas/frases secretas do aplicativo e do sistema contra o uso indevido:
• Com que segurança as senhas/frases secretas são armazenadas (por exemplo, se estão armazenadas em um cofre de senhas).
• Rotatividade de pessoal.
• O número de pessoas com acesso ao fator de autenticação.
• Se a conta pode ser usada para login interativo.
• Se a postura de segurança das contas é analisada dinamicamente e se o acesso em tempo real aos recursos é determinado automaticamente (consulte o Requisito 8.3.9).
Todos esses elementos afetam o nível de risco para o aplicativo e as contas do sistema e podem afetar a segurança dos sistemas acessados pelo sistema e pelas contas do aplicativo.

(continua na página a seguir)</td></tr>
<tr><td rowspan="2">8.6.3 As senhas/frases secretas para qualquer aplicativo e contas do sistema são protegidas contra o uso indevido da seguinte forma:
• 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.</td><td>8.6.3.a Examine as políticas e procedimentos para verificar se os procedimentos são definidos para proteger senhas/frases secretas para aplicativos ou contas de sistema contra uso indevido, de acordo com todos os elementos especificados neste requisito.</td></tr>
<tr><td>8.6.3.b Examine a análise de risco direcionada da entidade para a frequência de mudança e complexidade para senhas/frases secretas usadas para login interativo para contas de aplicativo e sistema para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1 e endereça:
• A frequência definida para mudanças periódicas nas senhas/frases secretas do aplicativo e do sistema.
• A complexidade definida para senhas/frases secretas e adequação da complexidade em relação à frequência das alterações.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
As senhas/frases secretas usadas por contas de aplicativo e sistema não podem ser usadas indefinidamente e são estruturadas para resistir a ataques de força bruta e adivinhação.

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.</td><td>8.6.3.c Entreviste a equipe responsável e examine as definições de configuração do sistema para verificar se as senhas/frases secretas para qualquer aplicativo e contas do sistema que podem ser usadas para login interativo estão protegidas contra uso indevido de acordo com todos os elementos especificados neste requisito.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
		As entidades devem correlacionar sua frequência de alteração selecionada para aplicativos e senhas/senhas do sistema com sua complexidade selecionada para essas senhas/frases secretas - ou seja, a complexidade deve ser mais rigorosa quando as senhas/frases secretas são alteradas com pouca frequência e pode ser menos rigorosa quando alteradas com mais frequência. Por exemplo, uma frequência de alteração mais longa é mais justificável quando a complexidade das senhas/frases secretas é definida para 36 caracteres alfanuméricos com letras maiúsculas e minúsculas, números e caracteres especiais. As práticas recomendadas são considerar alterações de senha pelo menos uma vez por ano, um comprimento de senha/frase secreta de pelo menos 15 caracteres e complexidade para as senhas/frase secreta de caracteres alfanuméricos, com letras maiúsculas e minúsculas e caracteres especiais. **Informações Adicionais** Para obter informações sobre a variabilidade e equivalência de força da senha para senhas/frases secretas de formatos diferentes, consulte os padrões da indústria (por exemplo, a versão atual do *NIST SP 800-63 Digital Identity Guidelines).*

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

Seções	
9.1	Os processos e mecanismos para restringir o acesso físico aos dados do titular são definidos e compreendidos.
9.2	Os controles de acesso físico gerenciam a entrada em instalações e sistemas que contêm dados do titular do cartão.
9.3	O acesso físico para pessoal e visitantes é autorizado e gerenciado.
9.4	A mídia com os dados do titular do cartão é armazenada, acessada, distribuída e destruída com segurança.
9.5	Dispositivos de ponto de interação (POI) são protegidos contra adulteração e substituição não autorizada.

Visão Geral

Qualquer acesso físico aos dados do titular do cartão ou sistemas que armazenam, processam ou transmitem os dados do titular do cartão oferece aos indivíduos a oportunidade de acessar e/ou remover sistemas ou cópias impressas contendo os dados do titular do cartão; portanto, o acesso físico deve ser adequadamente restrito.

Existem três áreas diferentes mencionadas no Requisito 9:

1. Os requisitos que se referem especificamente a áreas sensíveis devem ser aplicados apenas a essas áreas.
2. Os requisitos que se referem especificamente ao ambiente de dados do titular do cartão (CDE) se aplicam a todo o CDE, incluindo quaisquer áreas sensíveis que residam no CDE.
3. Os requisitos que se referem especificamente à instalação estão referenciando os tipos de controles que podem ser gerenciados de forma mais ampla no limite físico de uma localização de negócios (como um edifício) dentro da qual residem CDEs e áreas sensíveis. Esses controles geralmente existem fora de um CDE ou área sensível, por exemplo, uma mesa de guarda que identifica, atribui crachá e registra visitantes. O termo “instalação” é usado para reconhecer que esses controles podem existir em diferentes locais dentro de uma instalação, por exemplo, na entrada do prédio ou na entrada interna de um data center ou espaço de escritório.

Consulte o Apêndice G para obter as definições de “Mídias”, “Pessoal”, “Área Sensível” e outros termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
9.1 Os processos e mecanismos para restringir o acesso físico aos dados do titular do cartão são definidos e compreendidos.		
Requisitos da Abordagem Definida **9.1.1** Todas as políticas e processos operacionais identificados no Requisito 9 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 9 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **9.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 9 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 9.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 9. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 9, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política. Políticas e procedimentos, incluindo atualizações, são comunicados ativamente a todo o pessoal afetado e são apoiados por procedimentos operacionais que descrevem como realizar as atividades.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem designadas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
9.1.2 As funções e responsabilidades para a execução de atividades no Requisito 9 são documentadas, atribuídas e compreendidas.	**9.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 9 estão documentadas e atribuídas.	
	9.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 9 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 9 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
9.2 Os controles de acesso físico gerenciam a entrada em instalações e sistemas que contêm dados do titular do cartão.		
Requisitos da Abordagem Definida **9.2.1** Controles apropriados de entrada nas instalações estão implementados para restringir o acesso físico aos sistemas no CDE. **Objetivo da Abordagem Personalizada** Os componentes de sistema no CDE não podem ser acessados fisicamente por pessoal não autorizado.	**Procedimentos de Teste da Abordagem Definida** **9.2.1** Observe os controles de entrada e entreviste o pessoal responsável para verificar se os controles de segurança física estão implementados para restringir o acesso aos sistemas no CDE.	**Objetivo** Sem controles de acesso físico, pessoas não autorizadas podem potencialmente obter acesso ao CDE e informações confidenciais, ou podem alterar as configurações do sistema, introduzir vulnerabilidades na rede ou destruir ou roubar equipamentos. Portanto, o objetivo deste requisito é que o acesso físico ao CDE seja controlado por meio de controles de segurança física, como leitores de crachás ou outros mecanismos, como fechadura e chave. **Práticas Recomendadas** Qualquer que seja o mecanismo que atenda a este requisito, deve ser suficiente para a organização verificar se apenas o pessoal autorizado tem acesso concedido. **Exemplos** Os controles de entrada das instalações incluem controles de segurança física em cada sala de computadores, data center e outras áreas físicas com sistemas no CDE. Também pode incluir leitores de crachás ou outros dispositivos que gerenciam controles de acesso físico, como fechadura e chave com uma lista atual de todos os indivíduos que possuem as chaves.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**9.2.1.1.a** Observe a localização onde o ocorre acesso de pessoas às áreas sensíveis dentro do CDE para verificar se as câmeras de vídeo ou os mecanismos de controle de acesso físico (ou ambos) estão instalados para monitorar os pontos de entrada e saída. **9.2.1.1.b** Observe as localizações onde ocorre o acesso de pessoas às áreas sensíveis dentro do CDE para verificar se as câmeras de vídeo ou os mecanismos de controle de acesso físico (ou ambos) estão protegidos contra adulteração ou desativação. **9.2.1.1.c** Observe os mecanismos de controle de acesso físico e/ou examine as câmeras de vídeo e entreviste o pessoal responsável para verificar se: • Os dados coletados de câmeras de vídeo e/ou mecanismos de controle de acesso físico são revisados e correlacionados com outras entradas. • Os dados coletados são armazenados por pelo menos três meses.	Manter os detalhes das pessoas que entram e saem das áreas sensíveis pode ajudar nas investigações de violações físicas, identificando as pessoas que acessaram fisicamente as áreas sensíveis, bem como quando entraram e saíram. **Práticas Recomendadas** Qualquer que seja o mecanismo que atenda a esse requisito, ele deve monitorar com eficácia todos os pontos de entrada e saída de áreas sensíveis. Os criminosos que tentam obter acesso físico a áreas sensíveis geralmente tentam desativar ou contornar os controles de monitoramento. Para proteger esses controles de adulteração, as câmeras de vídeo podem ser posicionadas de forma que fiquem fora de alcance e/ou monitoradas para detectar adulteração. Da mesma forma, os mecanismos de controle de acesso físico podem ser monitorados ou ter proteções físicas instaladas para evitar que sejam danificados ou desativados por indivíduos mal-intencionados.
Objetivo da Abordagem Personalizada		
Registros confiáveis e verificáveis são mantidos de entrada e saída física individual de áreas confidenciais.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **9.2.2** Controles físicos e/ou lógicos são implementados para restringir o uso de tomadas de rede acessíveis ao público dentro da instalação. **Objetivo da Abordagem Personalizada** Dispositivos não autorizados não podem se conectar à rede da entidade a partir de áreas públicas dentro das instalações.	**Procedimentos de Teste da Abordagem Definida** **9.2.2** Entreviste o pessoal responsável e observe a localização das tomadas de rede acessíveis ao público para verificar se os controles físicos e/ou lógicos estão em vigor para restringir o acesso às tomadas de rede acessíveis ao público dentro da instalação.	**Objetivo** Restringir o acesso às tomadas de rede (ou portas de rede) impedirá que indivíduos mal-intencionados se conectem a tomadas de rede prontamente disponíveis e tenham acesso ao CDE ou aos sistemas conectados ao CDE. **Práticas Recomendadas** Sejam controles lógicos ou físicos, ou uma combinação de ambos, eles devem impedir que um indivíduo ou dispositivo que não esteja explicitamente autorizado seja capaz de se conectar à rede. **Exemplos** Os métodos para atender a esse requisito incluem desativar as tomadas de rede localizadas em áreas públicas e áreas acessíveis aos visitantes e ativar apenas quando o acesso à rede for explicitamente autorizado. Como alternativa, processos podem ser implementados para garantir que os visitantes sejam acompanhados o tempo todo nas áreas com tomadas de rede ativas.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** O equipamento de rede física não pode ser acessado por pessoal não autorizado.	**Procedimentos de Teste da Abordagem Definida** **9.2.3** Entreviste o pessoal responsável e observe os locais de hardware e linhas para verificar se o acesso físico a pontos de acesso wireless, gateways, hardware de rede/comunicação e linhas de telecomunicações dentro da instalação é restrito.	**Objetivo** Sem a segurança física adequada sobre o acesso a componentes wireless e dispositivos de rede de computadores e equipamentos e linhas de telecomunicações, usuários mal-intencionados podem obter acesso aos recursos de rede da entidade. Além disso, eles podem conectar seus próprios dispositivos à rede para obter acesso não autorizado ao CDE ou aos sistemas conectados ao CDE. Além disso, proteger o hardware de rede e comunicação evita que usuários mal-intencionados interceptem o tráfego da rede ou conectem fisicamente seus próprios dispositivos a recursos de rede com fio.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
9.2.4 O acesso aos consoles em áreas sensíveis é restrito por meio de bloqueio quando não estiver em uso.	**9.2.4** Observe a tentativa de um administrador de sistema de fazer logon em consoles em áreas sensíveis e verifique se eles estão "bloqueados" para evitar o uso não autorizado.	O bloqueio das telas de login do console evita que pessoas não autorizadas obtenham acesso a informações confidenciais, alterando as configurações do sistema, introduzindo vulnerabilidades na rede ou destruindo registros.
Objetivo da Abordagem Personalizada		
Os consoles físicos em áreas sensíveis não podem ser usados por pessoal não autorizado.		

Requisitos e Procedimentos de Teste		Diretriz
9.3 O acesso físico para pessoal e visitantes é autorizado e gerenciado.		
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os requisitos para acesso ao CDE físico são definidos e aplicados para identificar e autorizar o pessoal.	**Procedimentos de Teste da Abordagem Definida** **9.3.1.a** Examine os procedimentos documentados para verificar se os procedimentos para autorizar e gerenciar o acesso físico do pessoal ao CDE são definidos de acordo com todos os elementos especificados neste requisito. **9.3.1.b** Observe os métodos de identificação, como crachás de identificação e os processos para verificar se o pessoal no CDE está claramente identificado. **9.3.1.c** Observe o processo para verificar o acesso ao processo de identificação, como um sistema de crachás, é limitado ao pessoal autorizado.	**Objetivo** Estabelecer procedimentos para conceder, gerenciar e remover o acesso quando não for mais necessário garante que indivíduos não autorizados sejam impedidos de obter acesso às áreas que contêm dados do titular do cartão. Além disso, é importante limitar o acesso ao sistema de crachás e aos crachás para evitar que pessoas não autorizadas façam seus próprios crachás e/ou estabeleçam suas próprias regras de acesso. **Práticas Recomendadas** É importante identificar visualmente o pessoal que está fisicamente presente e se o indivíduo é um visitante ou um funcionário. **Exemplos** Uma forma de identificar o pessoal é atribuir crachás a eles.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="4">Objetivo
Controlar o acesso físico a áreas confidenciais ajuda a garantir que apenas o pessoal autorizado com uma necessidade de negócios legítima tenha acesso concedido.
Práticas Recomendadas
Sempre que possível, as organizações devem ter políticas e procedimentos para garantir que, antes de o pessoal deixar a organização, todos os mecanismos de acesso físico sejam devolvidos ou desativados o mais rápido possível após sua partida. Isso irá garantir que o pessoal não tenha acesso físico a áreas sensíveis, uma vez que seu emprego tenha terminado.</td></tr>
<tr><td rowspan="2">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 desligamento.
• Todos os mecanismos de acesso físico, como chaves, cartões de acesso, etc., são devolvidos ou desabilitados no desligamento.</td><td>9.3.1.1.a Observe o pessoal em áreas sensíveis dentro do CDE, entreviste o pessoal responsável e examine as listas de controle de acesso físico para verificar se:
• O acesso à área sensível é autorizado.
• O acesso é necessário para a função de trabalho do indivíduo.</td></tr>
<tr><td>9.3.1.1.b Observe os processos e entreviste o pessoal para verificar se o acesso de todo o pessoal é revogado imediatamente após o desligamento.</td></tr>
<tr><td>Objetivo da Abordagem Personalizada
As áreas sensíveis não podem ser acessadas por pessoal não autorizado.</td><td>9.3.1.1.c Para pessoal desligado, examine as listas de controle de acesso físico e entreviste o pessoal responsável para verificar se todos os mecanismos de acesso físico (como chaves, cartões de acesso, etc.) foram devolvidos ou desativados.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**9.3.2.a** Examine os procedimentos documentados e entreviste o pessoal para verificar se os procedimentos estão definidos para autorizar e gerenciar o acesso de visitantes ao CDE de acordo com todos os elementos especificados neste requisito.	Os controles de visitantes são importantes para reduzir a capacidade de pessoas não autorizadas e mal-intencionadas de obter acesso às instalações e, potencialmente, aos dados do titular do cartão. Os controles de visitantes garantem que os visitantes sejam identificáveis como visitantes, para que o pessoal possa monitorar suas atividades e que seu acesso seja restrito apenas à duração de sua visita legítima.
	9.3.2.b Observe os processos quando os visitantes estão presentes no CDE e entreviste o pessoal para verificar se os visitantes estão: • Autorizados antes de entrar no CDE. • Acompanhados em todos os momentos dentro do CDE.	
	9.3.2.c Observe o uso de crachás de visitante ou outra identificação para verificar se o crachá ou outra identificação não permite o acesso sem escolta ao CDE.	
	9.3.2.d Observe os visitantes no CDE para verificar se: • Crachás de visitante ou outra identificação estão sendo usados para todos os visitantes. • Crachás de visitante ou identificação facilmente distinguem visitantes de funcionários.	
Objetivo da Abordagem Personalizada	**9.3.2.e** Examine os crachás de visitante ou outra identificação e observe as evidências no sistema de crachás para verificar se os crachás de visitante ou outra identificação expiram.	
Os requisitos para o acesso do visitante ao CDE são definidos e aplicados. Os visitantes não podem exceder qualquer acesso físico autorizado permitido enquanto no CDE.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **9.3.3** Crachás ou identificação de visitante são entregues ou desativados antes dos visitantes deixarem as instalações ou na data de expiração. **Objetivo da Abordagem Personalizada** A identificação do visitante ou os crachás não podem ser reutilizados após o vencimento.	**Procedimentos de Teste da Abordagem Definida** **9.3.3** Observe os visitantes que saem das instalações e entreviste os funcionários para verificar se os crachás de visitante ou outra identificação foram entregues ou desativados antes dos visitantes deixarem as instalações ou na data de expiração.	**Objetivo** Garantir que os crachás de visitante sejam devolvidos ou desativados após o término ou conclusão da visita evita que pessoas mal-intencionadas usem um passe previamente autorizado para obter acesso físico ao prédio após o término da visita.
Requisitos da Abordagem Definida **9.3.4** Um registro de visitantes é usado para manter um registro físico da atividade do visitante dentro da instalação e 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 de outra forma restrito por lei. **Objetivo da Abordagem Personalizada** Registros de acesso de visitantes que permitem a identificação de indivíduos são mantidos	**Procedimentos de Teste da Abordagem Definida** **9.3.4.a** Examine o registro de visitantes e entreviste o pessoal responsável para verificar se um registro de visitantes é usado para registrar o acesso físico às instalações e áreas sensíveis. **9.3.4.b** Examine o registro do visitante e verifique se o registro contém: • O nome do visitante e a organização representada. • O pessoal que autoriza o acesso físico. • Data e hora da visita. **9.3.4.c** Examine os locais de armazenamento dos registros de visitantes e entreviste os funcionários responsáveis para verificar se o registro é retido por pelo menos três meses, a menos que de outra forma restrito por lei.	**Objetivo** Um registro de visitantes documentando informações mínimas sobre o visitante é fácil e barato de manter. Isso ajudará a identificar o histórico de acesso físico a um edifício ou sala e o acesso potencial aos dados do titular do cartão. **Práticas Recomendadas** Ao registrar a data e a hora da visita, incluir os horários de entrada e saída é considerada uma prática recomendada, pois fornece informações úteis de rastreamento e garante que o visitante saiu no final do dia. Também é bom verificar se o ID de um visitante (carteira de motorista, etc.) corresponde ao nome que ele colocou no registro de visitante.

Requisitos e Procedimentos de Teste		Diretriz
9.4 A mídia com os dados do titular do cartão é armazenada, acessada, distribuída e destruída com segurança.		
Requisitos da Abordagem Definida **9.4.1** Todas as mídias com dados do titular do cartão estão seguras fisicamente. **Objetivo da Abordagem Personalizada** A mídia com dados do titular do cartão não pode ser acessada por pessoal não autorizado.	**Procedimentos de Teste da Abordagem Definida** **9.4.1** Examine a documentação para verificar se os procedimentos definidos para proteger os dados do titular do cartão incluem os controles para a segurança física de todas as mídias.	**Objetivo** Os controles para proteger fisicamente a mídia têm o objetivo de impedir que pessoas não autorizadas tenham acesso aos dados do titular do cartão em qualquer mídia. Os dados do titular do cartão estão sujeitos à visualização, cópia ou digitalização não autorizada se estiverem desprotegidos enquanto estiverem em uma mídia removível ou portátil, impressos ou deixados na mesa de alguém.
9.4.1.1 Os backups em mídia off-line com os dados do titular do cartão são armazenados em um local seguro. **Objetivo da Abordagem Personalizada** Os backups off-line não podem ser acessados por pessoal não autorizado.	**9.4.1.1.a** Examine a documentação para verificar se os procedimentos estão definidos para proteger fisicamente backups em mídia off-line com os dados do titular do cartão em um local seguro. **9.4.1.1.b** Examine os registros ou outra documentação e entreviste a equipe responsável no local de armazenamento para verificar se os backups em mídia off-line estão armazenados em um local seguro.	**Objetivo** Se armazenados em uma instalação não protegida, os backups contendo os dados do titular do cartão podem ser facilmente perdidos, roubados ou copiados com más intenções. **Práticas Recomendadas** Para o armazenamento seguro da mídia de backup, uma boa prática é armazenar a mídia em um local externo, como um local alternativo ou de backup ou local de armazenamento comercial.
Requisitos da Abordagem Definida **9.4.1.2** A segurança do(s) local(is) com backup em mídia off-line contendo os dados do titular do cartão é revisada pelo menos uma vez a cada 12 meses. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **9.4.1.2.a** Examine a documentação para verificar se os procedimentos são definidos para revisar a segurança do(s) local(is) com backup em mídia off-line contendo os dados do titular do cartão, pelo menos uma vez a cada 12 meses.	**Objetivo** A realização de análises regulares das instalações de armazenamento permite que a organização resolva os problemas de segurança identificados imediatamente, minimizando o risco potencial. É importante que a entidade esteja ciente da segurança da área onde a mídia está sendo armazenada.

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Os controles de segurança que protegem os backups off-line são verificados periodicamente por inspeção.	**9.4.1.2.b** Examine os procedimentos documentados, registros ou outra documentação e entreviste o pessoal responsável no(s) local(is) de armazenamento para verificar se a segurança do local de armazenamento é revisada pelo menos uma vez a cada 12 meses.	
Requisitos da Abordagem Definida **9.4.2** Todas as mídias com dados do titular do cartão são classificadas de acordo com a confidencialidade dos dados.	**Procedimentos de Teste da Abordagem Definida** **9.4.2.a** Examine a documentação para verificar se os procedimentos são definidos para classificar a mídia com os dados do titular do cartão de acordo com a confidencialidade dos dados.	**Objetivo** A mídia não identificada como confidencial pode não ser protegida adequadamente ou pode ser perdida ou roubada. **Práticas Recomendadas** É importante que a mídia seja identificada de forma que seu status de classificação seja aparente. Isso não significa, entretanto, que a mídia precisa ter um rótulo “confidencial”.
	9.4.2.b Examine os registros de mídia ou outra documentação para verificar se todas as mídias estão classificadas de acordo com a confidencialidade dos dados.	
Objetivo da Abordagem Personalizada As mídias são classificadas e protegidas de forma adequada.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 transporte seguro ou outro método de entrega que possa ser rastreada com precisão. Os registros de rastreamento externo incluem detalhes sobre a localização da mídia.	**9.4.3.a** Examine a documentação para verificar se os procedimentos estão definidos para proteger a mídia enviada para fora da instalação de acordo com todos os elementos especificados neste requisito.	A mídia pode ser perdida ou roubada se enviada por um método não rastreável, como o correio normal. O uso de transportes seguros para entregar qualquer mídia que contenha dados do titular do cartão permite que as organizações usem seus sistemas de rastreamento para manter o estoque e a localização das remessas.
	9.4.3.b Entreviste a equipe e examine os registros para verificar se toda a mídia enviada para fora da instalação é registrada e enviada por meio de transporte seguro ou outro método de entrega que possa ser rastreado.	
Objetivo da Abordagem Personalizada	**9.4.3.c** Examine os registros de rastreamento externo para todas as mídias para verificar se os detalhes de rastreamento estão documentados.	
A mídia é protegida e rastreada quando transportada para fora das instalações.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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).	**9.4.4.a** Examine a documentação para verificar se os procedimentos estão definidos para garantir que a mídia movida para fora da instalação seja aprovada pela gerência.	Sem um processo firme para garantir que todos os movimentos de mídia sejam aprovados antes que a mídia seja removida das áreas seguras, a mídia não seria rastreada ou protegida adequadamente e sua localização seria desconhecida, levando à perda ou furto de mídia.
	9.4.4.b Examine os registros de rastreamento de mídia externa e entreviste o pessoal responsável para verificar se a autorização pela gerência adequada foi obtida para todas as mídias movidas para fora das instalações (incluindo mídia distribuída a indivíduos).	
Objetivo da Abordagem Personalizada		
A mídia não pode deixar uma instalação sem a aprovação de pessoal responsável.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Os indivíduos que aprovam movimentos de mídia devem ter o nível apropriado de autoridade administrativa para conceder essa aprovação. No entanto, não é especificamente exigido que tais indivíduos tenham "gerente" como parte de seu cargo.		
Requisitos da Abordagem Definida **9.4.5** Registros de inventário de todas as mídias eletrônicas com os dados do titular do cartão são mantidos. **Objetivo da Abordagem Personalizada** São mantidos inventários precisos de mídia eletrônica armazenada.	**Procedimentos de Teste da Abordagem Definida** **9.4.5.a** Examine a documentação para verificar se os procedimentos são definidos para manter registros de inventário de mídia eletrônica. **9.4.5.b** Examine os registros de inventário de mídia eletrônica e entreviste o pessoal responsável para verificar se os registros são mantidos.	**Objetivo** Sem métodos de inventário e controles de armazenamento cuidadosos, mídias eletrônicas roubadas ou perdidas podem passar despercebidas por um período indefinido de tempo.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os inventários de mídia são verificados periodicamente.	**Procedimentos de Teste da Abordagem Definida** **9.4.5.1.a** Examine a documentação para verificar se os procedimentos estão definidos para a realização de inventários de mídia eletrônica com os dados do titular do cartão pelo menos uma vez a cada 12 meses. **9.4.5.1.b** Examine os registros de inventário de mídia eletrônica e entreviste o pessoal para verificar se os inventários de mídia eletrônica são realizados pelo menos uma vez a cada 12 meses.	**Objetivo** Sem métodos de inventário e controles de armazenamento cuidadosos, mídias eletrônicas roubadas ou perdidas podem passar despercebidas por um período indefinido de tempo.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
9.4.6 Os materiais impressos com os dados do titular do cartão são destruídos quando não são mais necessários para o negócio ou razões legais, da seguinte forma: Os materiais são retalhados, incinerados ou transformados em polpa para que os dados do titular do cartão não possam ser reconstruídos. Os materiais são armazenados em recipientes de armazenamento seguro antes da destruição.	**9.4.6.a** Examine a política de destruição periódica de mídia para verificar se os procedimentos são definidos para destruir a mídia impressa com os dados do titular do cartão quando não forem mais necessários para o negócio ou razões legais, de acordo com todos os elementos especificados neste requisito.	Se não forem tomadas medidas para destruir as informações contidas na mídia impressa antes do descarte, indivíduos mal-intencionados podem recuperar as informações da mídia descartada, levando ao comprometimento dos dados. Por exemplo, indivíduos mal-intencionados podem usar uma técnica conhecida como *"dumpster diving"*, em que vasculham latas de lixo e lixeiras em busca de materiais impressos com informações que possam usar para lançar um ataque. Proteger os contêineres de armazenamento usados para materiais que serão destruídos evita que informações confidenciais sejam capturadas enquanto os materiais estão sendo coletados.
	9.4.6.b Observe os processos e entreviste o pessoal para verificar se os materiais impressos são cortados, fragmentados, incinerados ou transformados em polpa de forma que os dados do titular do cartão não possam ser reconstruídos.	**Práticas Recomendadas** Considere recipientes "a serem destruídos" com uma trava que impede o acesso ao seu conteúdo ou que fisicamente impede o acesso ao interior do recipiente.
Objetivo da Abordagem Personalizada Os dados do titular do cartão não podem ser recuperados da mídia que foi destruída ou cuja destruição está pendente.	**9.4.6.c** Observe os recipientes de armazenamento usados para materiais que contenham informações a serem destruídas para verificar se os recipientes são seguros.	**Informações Adicionais** Consulte *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*.
Observações de Aplicabilidade Esses requisitos para destruição de mídia quando essa mídia não é mais necessária para o negócio ou razões legais 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **9.4.7** A mídia eletrônica com os dados do titular do cartão é destruída quando não é mais necessária para o negócio ou razões legais 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. **Objetivo da Abordagem Personalizada** Os dados do titular do cartão não podem ser recuperados da mídia que foi apagada ou destruída. **Observações de Aplicabilidade** Esses requisitos para destruição de mídia quando essa mídia não é mais necessária para o negócio ou razões legais 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.	**Procedimentos de Teste da Abordagem Definida** **9.4.7.a** Examine a política de destruição de mídia periódica para verificar se os procedimentos são definidos para destruir a mídia eletrônica quando não for mais necessária para o negócio ou razões legais, de acordo com todos os elementos especificados neste requisito. **9.4.7.b** Observe o processo de destruição da mídia e entreviste o pessoal responsável para verificar se a mídia eletrônica com os dados do titular do cartão é destruída por um dos métodos especificados neste requisito.	**Objetivo** Se não forem tomadas medidas para destruir as informações contidas na mídia eletrônica quando não forem mais necessárias, indivíduos mal-intencionados podem recuperar informações da mídia descartada, levando ao comprometimento dos dados. Por exemplo, indivíduos mal-intencionados podem usar uma técnica conhecida como *"dumpster diving"*, em que vasculham latas de lixo e lixeiras em busca de informações que possam usar para lançar um ataque. **Práticas Recomendadas** A função de exclusão na maioria dos sistemas operacionais permite que os dados excluídos sejam recuperados, portanto, em vez disso, uma função ou aplicativo de exclusão seguro dedicado deve ser usado para tornar os dados irrecuperáveis. **Exemplos** Os métodos para destruir a mídia eletrônica com segurança incluem limpeza segura de acordo com os padrões aceitos pela indústria para exclusão segura, desmagnetização ou destruição física (como trituração ou fragmentação de discos rígidos). **Informações Adicionais** Consulte *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization.*

Requisitos e Procedimentos de Teste		Diretriz
9.5 Dispositivos de ponto de interação (POI) são protegidos contra adulteração e substituição não autorizada.		
Requisitos da Abordagem Definida **9.5.1** Dispositivos POI que capturam dados de cartão de pagamento por meio de interação física direta com a forma de 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. **Objetivo da Abordagem Personalizada** A entidade definiu procedimentos para proteger e gerenciar dispositivos de ponto de interação. As expectativas, controles e supervisão para o gerenciamento e proteção dos dispositivos POI são definidos e seguidos pelo pessoal afetado. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **9.5.1** Examine as políticas e procedimentos documentados para verificar se os processos definidos incluem todos os elementos especificados neste requisito.	**Objetivo** Os criminosos tentam roubar dados de cartões de pagamento roubando e/ou manipulando dispositivos e terminais de leitura de cartões. Os criminosos tentam roubar dispositivos para aprender como invadi-los e, muitas vezes, tentam substituir dispositivos legítimos por dispositivos fraudulentos que enviam dados de cartão de pagamento sempre que um cartão é inserido. Eles também tentarão adicionar componentes de "skimming" na parte externa dos dispositivos, que são projetados para capturar dados do cartão de pagamento antes que eles entrem no dispositivo - por exemplo, conectando um leitor de cartão adicional em cima do leitor de cartão legítimo para que os dados do cartão de pagamento sejam capturados duas vezes: uma pelo componente do criminoso e, em seguida, pelo componente legítimo do dispositivo. Dessa forma, as transações ainda podem ser concluídas sem interrupção enquanto o criminoso está "*skimming* [copiando]" os dados do cartão de pagamento durante o processo. **Informações Adicionais** As práticas recomendadas adicionais sobre prevenção de *skimming* estão disponíveis no site do PCI SSC.

Requisitos e Procedimentos de Teste		Diretriz
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). Este requisito não se destina a ser aplicado a componentes de entrada manual do PAN, como teclados de computador. Este requisito é recomendado, mas não obrigatório, para componentes de entrada manual do PAN, como teclados de computador. Este requisito não se aplica a 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.		
Requisitos da Abordagem Definida **9.5.1.1** Uma lista atualizada de dispositivos POI é mantida, incluindo: • Fabricante e modelo do dispositivo. • Localização do dispositivo. • Número de série do dispositivo ou outros métodos de identificação exclusiva.	**Procedimentos de Teste da Abordagem Definida** **9.5.1.1.a** Examine a lista de dispositivos POI para verificar se inclui todos os elementos especificados neste requisito. **9.5.1.1.b** Observe os dispositivos POI e as localizações dos dispositivos e compare com aqueles da lista para verificar se esta está precisa e atualizada. **9.5.1.1.c** Entreviste a equipe para verificar se a lista de dispositivos POI está atualizada quando os dispositivos são adicionados, realocados, desativados, etc.	**Objetivo** Manter uma lista atualizada de dispositivos POI ajuda uma organização a rastrear onde os dispositivos devem estar e identificar rapidamente se um dispositivo está faltando ou perdido. **Práticas Recomendadas** O método para manter uma lista de dispositivos pode ser automatizado (por exemplo, um sistema de gerenciamento de dispositivo) ou manual (por exemplo, documentado em registros eletrônicos ou em papel). Para dispositivos em movimento, a localização pode incluir o nome da equipe a quem o dispositivo foi atribuído. **Exemplos** Os métodos para manter a localização dos dispositivos incluem a identificação do endereço do local ou instalação onde o dispositivo está localizado.
Objetivo da Abordagem Personalizada A identidade e a localização dos dispositivos POI são gravadas e conhecidas em todos os momentos.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
9.5.1.2 As superfícies do dispositivo POI são inspecionadas periodicamente para detectar adulteração e substituição não autorizada.	**9.5.1.2.a** Examine os procedimentos documentados para verificar se os processos são definidos para as inspeções periódicas das superfícies do dispositivo POI para detectar adulteração e substituição não autorizada.	**Objetivo** As inspeções regulares de dispositivos ajudarão as organizações a detectar adulteração mais rapidamente por meio de evidências externas - por exemplo, a adição de um skimmer de cartão - ou a substituição de um dispositivo, minimizando assim o impacto potencial do uso de dispositivos fraudulentos. **Práticas Recomendadas** Os métodos de inspeção periódica incluem verificar o número de série ou outras características do dispositivo e comparar as informações com a lista de dispositivos POI para verificar se o dispositivo não foi trocado por um dispositivo fraudulento. **Exemplos** O tipo de inspeção dependerá do dispositivo. Por exemplo, fotografias de dispositivos sabidamente seguros podem ser usadas para comparar a aparência atual de um dispositivo com sua aparência original para ver se ele mudou. Outra opção pode ser usar uma caneta marcadora segura, como um marcador de luz ultravioleta, para marcar as superfícies do dispositivo e as aberturas do dispositivo para que qualquer violação ou substituição seja aparente. Os criminosos frequentemente substituem o revestimento externo de um dispositivo para ocultar sua adulteração, e esses métodos podem ajudar a detectar tais atividades. Os fornecedores de dispositivos também podem fornecer orientações de segurança e guias para ajudar a determinar se o dispositivo está sujeito à adulteração. *(continua na página a seguir)*
	9.5.1.2.b Entreviste o pessoal responsável e observe os processos de inspeção para verificar: • O pessoal está ciente dos procedimentos de inspeção de dispositivos. • Todos os dispositivos são inspecionados periodicamente em busca de evidências de adulteração e substituição não autorizada.	

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td colspan="2">Objetivo da Abordagem Personalizada

Os dispositivos de ponto de interação não podem ser adulterados, substituídos sem autorização ou ter dispositivos de skimming instalados sem detecção oportuna.</td><td rowspan="2">Os sinais de que um dispositivo pode ter sido adulterado ou substituído incluem:
• Conexões inesperadas ou cabos conectados ao dispositivo.
• Etiquetas de segurança ausentes ou alteradas.
• Caixa quebrada ou com cores diferentes.
• Alterações no número de série ou outras marcações externas.</td></tr>
<tr><td>Requisitos da Abordagem Definida

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.

Objetivo da Abordagem Personalizada

Os dispositivos POI são inspecionados com uma frequência que aborda o risco da entidade.

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.</td><td>Procedimentos de Teste da Abordagem Definida

9.5.1.2.1.a Examine a análise de risco direcionada da entidade para a frequência das inspeções periódicas do dispositivo POI e o tipo de inspeções realizadas para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1.

9.5.1.2.1.b Examine os resultados documentados das inspeções periódicas do dispositivo e entreviste o pessoal para verificar se a frequência e o tipo de inspeções do dispositivo POI realizadas correspondem ao que está definido na análise de risco direcionada da entidade conduzida para este requisito.</td><td>Objetivo

As entidades estão em melhor posição para determinar a frequência das inspeções do dispositivo POI com base no ambiente em que o dispositivo opera.

Práticas Recomendadas

A frequência das inspeções dependerá de fatores como a localização de um dispositivo e se o dispositivo é assistido ou não. Por exemplo, dispositivos deixados em áreas públicas sem supervisão do pessoal da organização podem ter inspeções mais frequentes do que dispositivos mantidos em áreas seguras ou supervisionados quando acessíveis ao público. Além disso, muitos fornecedores de POI incluem orientação em sua documentação do usuário sobre a frequência com que os dispositivos de POI devem ser verificados e para quê - as entidades devem consultar a documentação de seus fornecedores e incorporar essas recomendações em suas inspeções periódicas.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 nos 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.	**9.5.1.3.a** Revise os materiais de treinamento para o pessoal em ambientes de POI para verificar se eles incluem todos os elementos especificados neste requisito. **9.5.1.3.b** Entreviste o pessoal em ambientes de POI para verificar se eles receberam treinamento e conhecer os procedimentos para todos os elementos especificados neste requisito**.**	Os criminosos costumam se passar por pessoal de manutenção autorizado para obter acesso aos dispositivos POI. **Práticas Recomendadas** O treinamento de pessoal deve incluir estar alerta e questionar qualquer pessoa que apareça para fazer a manutenção do POI para garantir que está autorizado e tem uma ordem de serviço válida, incluindo quaisquer agentes, pessoal de manutenção ou reparo, técnicos, prestadores de serviços ou outros terceiros. Todos os terceiros que solicitam acesso aos dispositivos devem sempre ser verificados antes de receber o acesso - por exemplo, verificando com a gerência ou telefonando para a empresa de manutenção do POI, como o fornecedor ou adquirente, para verificação. Muitos criminosos tentarão enganar o pessoal vestindo-se para o papel (por exemplo, carregando caixas de ferramentas e vestidos com roupas de trabalho) e também podem ter conhecimento sobre a localização dos dispositivos, portanto, o pessoal deve ser treinado para sempre seguir os procedimentos. Outro truque que os criminosos usam é enviar um "novo" dispositivo POI com instruções para trocá-lo por um dispositivo legítimo e "devolver" o dispositivo legítimo. Os criminosos podem até fornecer postagem de retorno para o endereço especificado. Portanto, a equipe deve sempre verificar com seu gerente ou fornecedor se o dispositivo é legítimo e vem de uma fonte confiável antes de instalá-lo ou usá-lo para negócios. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
O pessoal está bem informado sobre os tipos de ataques contra dispositivos POI, as contramedidas técnicas e de procedimentos da entidade e podem acessar assistência e orientação quando necessário.		

Requisitos e Procedimentos de Teste		Diretriz
		Exemplos O comportamento suspeito que o pessoal deve estar ciente inclui tentativas de pessoas desconhecidas de desconectar ou abrir dispositivos. Garantir que o pessoal esteja ciente dos mecanismos para relatar comportamento suspeito e a quem relatar tal comportamento - por exemplo, um gerente ou oficial de segurança - ajudará a reduzir a probabilidade e o impacto potencial de um dispositivo ser adulterado ou substituído.

Monitorar e Testar as Redes Regularmente

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

Seções	
10.1	Processos e mecanismos para registrar e monitorar todos os acessos aos componentes de sistema e aos dados do titular do cartão são definidos e documentados.
10.2	Os registros de auditoria são implementados para apoiar a detecção de anomalias e atividades suspeitas, e a análise forense de eventos.
10.3	Os registros de auditoria são protegidos contra destruição e modificações não autorizadas.
10.4	Os registros de auditoria são revisados para identificar anomalias ou atividades suspeitas.
10.5	O histórico do registro de auditoria é mantido e disponível para análise.
10.6	Os mecanismos de sincronização de tempo suportam configurações de tempo consistentes em todos os sistemas.
10.7	Falhas de sistemas críticos de controle de segurança são detectadas, relatadas e respondidas prontamente.

Visão Geral

Os mecanismos de registro e a capacidade de rastrear as atividades do usuário são essenciais para prevenir, detectar ou minimizar o impacto do comprometimento dos dados. A presença de registros em todos os componentes de sistema e no ambiente de dados do titular do cartão (CDE) permite rastreamento, alerta e análise completos quando algo dá errado. Determinar a causa de um comprometimento é difícil, senão impossível, sem os registros de atividade do sistema.

Este requisito se aplica às atividades do usuário, incluindo aquelas realizadas por funcionários, contratados, consultores e fornecedores internos e externos e outros terceiros (por exemplo, aqueles que fornecem serviços de suporte ou manutenção).

Esses requisitos não se aplicam à atividade do usuário de consumidores (titulares de cartão).

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
10.1 Processos e mecanismos para registrar e monitorar todos os acessos aos componentes de sistema e aos dados do titular do cartão são definidos e documentados.		
Requisitos da Abordagem Definida **10.1.1** Todas as políticas e processos operacionais identificados no Requisito 10 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 10 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **10.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais identificados no Requisito 10 são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 10.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 10. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 10, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
10.1.2 As funções e responsabilidades para a execução de atividades no Requisito 10 são documentadas, atribuídas e compreendidas.	**10.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 10 estão documentadas e atribuídas.	
	10.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 10 para verificar se as funções e responsabilidades são atribuídas conforme são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 10 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
10.2 Os registros de auditoria são implementados para apoiar a detecção de anomalias e atividades suspeitas, e a análise forense de eventos.		
Requisitos da Abordagem Definida **10.2.1** Os registros de auditoria estão habilitados e ativos para todos os componentes de sistema e dados do titular do cartão. **Objetivo da Abordagem Personalizada** Registros de todas as atividades que afetam os componentes de sistema e os dados do titular do cartão são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1** Entreviste o administrador do sistema e examine as configurações do sistema para verificar se os registros de auditoria estão habilitados e ativos para todos os componentes de sistema.	**Objetivo** Os registros de auditoria deve existir para todos os componentes de sistema. Os registros de auditoria enviam alertas ao administrador do sistema, fornecem dados para outros mecanismos de monitoramento, como sistemas de detecção de intrusão (IDS) e sistemas de monitoramento de eventos e informações de segurança (SIEM), e fornecem uma trilha de histórico para investigação pós-incidente. Registrar e analisar eventos relevantes para a segurança permitem que uma organização identifique e rastreie atividades potencialmente maliciosas. **Práticas Recomendadas** Quando uma entidade considera quais informações devem ser registradas em seus registros, é importante lembrar que as informações armazenadas em registros de auditoria são confidenciais e devem ser protegidas de acordo com os requisitos deste padrão. Deve-se tomar cuidado para armazenar apenas informações essenciais nos registros de auditoria para minimizar o risco.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **10.2.1.1** Os registros de auditoria capturam todos os acessos individuais do usuário aos dados do titular do cartão. **Objetivo da Abordagem Personalizada** Os registros de todos os acessos individuais do usuário aos dados do titular do cartão são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.1** Examine as configurações do registro de auditoria e os dados do registro para verificar se todos os acessos de usuários individuais aos dados do titular do cartão são registrados.	**Objetivo** É fundamental ter um processo ou sistema que vincule o acesso do usuário aos componentes de sistema acessados. Indivíduos mal-intencionados podem obter conhecimento de uma conta de usuário com acesso a sistemas no CDE, ou podem criar uma nova conta não autorizada para acessar os dados do titular do cartão. **Práticas Recomendadas** Um registro de todos os acessos individuais aos dados do titular do cartão pode identificar quais contas podem ter sido comprometidas ou utilizadas indevidamente.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Registros de todas as ações realizadas por indivíduos com privilégios elevados são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.2** Examine as configurações de registro de auditoria e dados de registro para verificar se todas as ações realizadas por qualquer indivíduo com acesso administrativo, incluindo qualquer uso interativo de aplicativos ou contas do sistema, são registradas.	**Objetivo** Contas com privilégios de acesso aumentados, como a conta de “administrador” ou “root”, têm o potencial de impactar significativamente a segurança ou a funcionalidade operacional de um sistema. Sem um registro das atividades realizadas, uma organização não pode rastrear quaisquer problemas resultantes de um erro administrativo ou uso indevido de privilégio de volta à ação e conta específicas. **Definições** Contas com acesso administrativo são aquelas atribuídas com privilégios ou habilidades específicas para essa conta para gerenciar sistemas, redes e/ou aplicativos. As funções ou atividades consideradas administrativas estão além das executadas por usuários regulares como parte das funções rotineiras de negócios.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **10.2.1.3** Os registros de auditoria capturam todo o acesso aos registros de auditoria. **Objetivo da Abordagem Personalizada** Registros de todos os acessos aos registros de auditoria são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.3** Examine as configurações do registro de auditoria e os dados do registro para verificar se o acesso a todos os registros de auditoria foi capturado.	**Objetivo** Usuários mal-intencionados geralmente tentam alterar os registros de auditoria para ocultar suas ações. Um registro de acesso permite que uma organização rastreie quaisquer inconsistências ou possível adulteração dos registros para uma conta individual. Fazer com que os registros identifiquem alterações, adições e exclusões nos registros de auditoria pode ajudar a reconstituir as etapas feitas por pessoal não autorizado.
Requisitos da Abordagem Definida **10.2.1.4** Os registros de auditoria capturam todas as tentativas de acesso lógico inválido. **Objetivo da Abordagem Personalizada** Registros de todas as tentativas de acesso inválidas são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.4** Examine as configurações do registro de auditoria e os dados do registro para verificar se as tentativas de acesso lógico inválidas foram capturadas.	**Objetivo** Indivíduos mal-intencionados costumam realizar várias tentativas de acesso nos sistemas almejados. Várias tentativas de login inválido podem ser uma indicação de tentativas de um usuário não autorizado de “força bruta” ou adivinhação de uma senha.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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 alterações, adições ou exclusões de contas com acesso administrativo. **Objetivo da Abordagem Personalizada** Registros de todas as mudanças nas credenciais de identificação e autenticação são capturados.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.5** Examine as configurações do registro de auditoria e os dados do registro para verificar se as mudanças nas credenciais de identificação e autenticação são capturadas de acordo com todos os elementos especificados neste requisito.	**Objetivo** O registro de alterações nas credenciais de autenticação (incluindo elevação de privilégios, acréscimos e exclusões de contas com acesso administrativo) fornece evidências residuais de atividades. Usuários mal-intencionados podem tentar manipular credenciais de autenticação para ignorá-los ou personificar uma conta válida.
Requisitos da Abordagem Definida **10.2.1.6** Os registros de auditoria capturam o seguinte: • Todas as inicializações de novos registros de auditoria e • Inicialização, parada ou pausa dos registros de auditoria existentes. **Objetivo da Abordagem Personalizada** Registros de todas as mudanças no status da atividade de registro de auditoria são capturados	**Procedimentos de Teste da Abordagem Definida** **10.2.1.6** Examine as configurações do registro de auditoria e os dados do registro para verificar se todos os elementos especificados neste requisito foram capturados.	**Objetivo** Desligar ou pausar os registros de auditoria antes de realizar atividades ilícitas é uma prática comum para usuários mal-intencionados que desejam evitar a detecção. A inicialização de registros de auditoria pode indicar que um usuário desabilitou a função de registro para ocultar suas ações.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **10.2.1.7** Os registros de auditoria capturam toda a criação e exclusão de objetos de nível de sistema.	**Procedimentos de Teste da Abordagem Definida** **10.2.1.7** Examine as configurações do registro de auditoria e os dados do registro para verificar se a criação e exclusão de objetos de nível de sistema foram capturados.	**Objetivo** O software malicioso, como malware, geralmente cria ou substitui objetos de nível de sistema no sistema de destino para controlar uma função ou operação específica nesse sistema. Registrando quando objetos de nível de sistema são criados ou excluídos, será mais fácil determinar se tais modificações foram autorizadas.
Objetivo da Abordagem Personalizada Registros de alterações que indicam que um sistema foi modificado em relação à funcionalidade pretendida são capturados.		
Requisitos da Abordagem Definida **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 falha. • Origem do evento. • Identidade ou nome dos dados afetados, componente de sistema, recurso ou serviço (por exemplo, nome e protocolo).	**Procedimentos de Teste da Abordagem Definida** **10.2.2** Entreviste a equipe e examine as configurações do registro e os dados do registro de auditoria para verificar se todos os elementos especificados neste requisito estão incluídos nas entradas do registro para cada evento auditável (de 10.2.1.1 a 10.2.1.7).	**Objetivo** Ao registrar esses detalhes para os eventos auditáveis em 10.2.1.1 a 10.2.1.7, um comprometimento potencial pode ser rapidamente identificado, com detalhes suficientes para facilitar o acompanhamento de atividades suspeitas.
Objetivo da Abordagem Personalizada Dados suficientes para serem capazes de identificar tentativas bem-sucedidas e malsucedidas e quem, o quê, quando, onde e como para cada evento listado no requisito 10.2.1 são capturados.		

Requisitos e Procedimentos de Teste		Diretriz
10.3 Os registros de auditoria são protegidos contra destruição e modificações não autorizadas.		
Requisitos da Abordagem Definida **10.3.1** O acesso de leitura aos arquivos de registros de auditoria é limitado àqueles com uma necessidade relacionada ao trabalho. **Objetivo da Abordagem Personalizada** Os registros de atividades armazenados não podem ser acessados por pessoal não autorizado.	**Procedimentos de Teste da Abordagem Definida** **10.3.1** Entreviste os administradores do sistema e examine as configurações e os privilégios do sistema para verificar se apenas os indivíduos com necessidades relacionadas ao trabalho têm acesso de leitura aos arquivos de registro de auditoria.	**Objetivo** Os arquivos de registro de auditoria contêm informações confidenciais e o acesso de leitura aos arquivos de registro deve ser limitado apenas àqueles com uma necessidade de negócios válida. Esse acesso inclui arquivos de registro de auditoria nos sistemas de origem, bem como em qualquer outro lugar onde estejam armazenados. **Práticas Recomendadas** A proteção adequada dos registros de auditoria inclui forte controle de acesso que limita o acesso aos registros com base apenas na "necessidade de conhecimento" e o uso de segregação física ou de rede para tornar os registros mais difíceis de localizar e modificar.
Requisitos da Abordagem Definida **10.3.2** Os arquivos de registros de auditoria são protegidos para evitar modificações por indivíduos. **Objetivo da Abordagem Personalizada** Os registros de atividades armazenados não podem ser modificados pelo pessoal.	**Procedimentos de Teste da Abordagem Definida** **10.3.2** Examine as configurações e privilégios do sistema e entreviste os administradores do sistema para verificar se os arquivos de registro de auditoria atuais estão protegidos contra modificações por indivíduos por meio de mecanismos de controle de acesso, segregação física e/ou segregação de rede.	**Objetivo** Frequentemente, um indivíduo mal-intencionado que entrou na rede tentará editar os registros de auditoria para ocultar sua atividade. Sem a proteção adequada dos registros de auditoria, sua completude, precisão e integridade não podem ser garantidas, e os registros de auditoria podem se tornar inúteis como uma ferramenta de investigação após um comprometimento. Portanto, os registros de auditoria devem ser protegidos nos sistemas de origem, bem como em qualquer outro lugar onde estejam armazenados. **Práticas Recomendadas** As entidades devem tentar evitar que os registros sejam expostos em locais acessíveis ao público.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **10.3.3** Os arquivos de registro de auditoria, incluindo aqueles para tecnologias externas, são prontamente copiados para um(ns) servidor(es) de registro interno(s) seguro(s) central(is) ou outra mídia de difícil modificação. **Objetivo da Abordagem Personalizada** Os registros de atividades armazenados são protegidos e preservados em um local central para evitar modificações não autorizadas.	**Procedimentos de Teste da Abordagem Definida** **10.3.3** Examine as configurações de backup ou arquivos de registro para verificar se os arquivos de registro de auditoria atuais, incluindo aqueles para tecnologias externas, são prontamente copiados para um servidor de registro interno seguro e central ou outra mídia difícil de modificar.	**Objetivo** O backup realizado prontamente dos registros em um servidor de registro centralizado ou mídia difícil de alterar mantém os registros protegidos, mesmo se o sistema que os gera for comprometido. Gravar registros de tecnologias externas, como wireless, controles de segurança de rede, DNS e servidores de e-mail, reduz o risco desses registros serem perdidos ou alterados. **Práticas Recomendadas** Cada entidade determina a melhor maneira de fazer backup dos arquivos de registro, seja por meio de um ou mais servidores de registro centralizados ou outra mídia segura. Os registros podem ser gravados diretamente, descarregados ou copiados de sistemas externos para o sistema interno seguro ou mídia.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os registros de atividades armazenados não podem ser modificados sem que um alerta seja gerado.	**Procedimentos de Teste da Abordagem Definida** **10.3.4** Examine as configurações do sistema, os arquivos monitorados e os resultados das atividades de monitoramento para verificar o uso do software de monitoramento da integridade dos arquivos ou de detecção de alterações nos registros de auditoria.	**Objetivo** Os sistemas de monitoramento de integridade de arquivo ou detecção de alterações verificam as alterações em arquivos críticos e notificam quando tais alterações são identificadas. Para fins de monitoramento de integridade de arquivo, uma entidade geralmente monitora arquivos que não mudam regularmente, mas quando mudados, indicam um possível comprometimento. **Práticas Recomendadas** O software usado para monitorar as alterações nos registros de auditoria deve ser configurado para fornecer alertas quando os dados ou arquivos de registro existentes forem alterados ou excluídos. No entanto, novos dados de registro adicionados a um registro de auditoria não devem gerar um alerta.

Requisitos e Procedimentos de Teste		Diretriz
10.4 Os registros de auditoria são revisados para identificar anomalias ou atividades suspeitas.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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 de sistema que armazenam, processam ou transmitem CHD e/ou SAD. • Registros de todos os componentes de sistema críticos. • Registros de todos os servidores e componentes de 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).	**10.4.1.a** Examine as políticas e procedimentos de segurança para verificar se os processos estão definidos para revisar todos os elementos especificados neste requisito pelo menos uma vez ao dia. **10.4.1.b** Observe os processos e entreviste o pessoal para verificar se todos os elementos especificados neste requisito são revisados pelo menos uma vez ao dia	**Objetivo** Muitas violações ocorrem meses antes de serem detectadas. As revisões regulares do registro significam que os incidentes podem ser identificados rapidamente e resolvidos de forma proativa. **Práticas Recomendadas** Verificar os registros diariamente (7 dias por semana, 365 dias por ano, incluindo feriados) minimiza o tempo e a exposição de uma violação potencial. Ferramentas de coleta, análise e alerta de registro, sistemas centralizados de gerenciamento de registro, analisadores de registro e sistemas de gerenciamento de eventos e informações de segurança (SIEM) são exemplos de ferramentas automatizadas que podem ser usadas para atender a esse requisito. A revisão diária de eventos de segurança – por exemplo, notificações ou alertas que identificam atividades suspeitas ou anômalas – bem como de registros de componentes de sistema críticos e registros de sistemas que executam funções de segurança, como firewalls, IDS/IPS, sistemas de monitoramento de integridade de arquivo (FIM), etc., é necessária para identificar problemas potenciais. A determinação de “evento de segurança” irá variar para cada organização e pode incluir considerações para o tipo de tecnologia, localização e função do dispositivo. As organizações também podem desejar manter uma linha de base do tráfego “normal” para ajudar a identificar comportamentos anômalos. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Atividades potencialmente suspeitas ou anômalas são rapidamente identificadas para minimizar o impacto.		Uma entidade que usa prestadores de serviços terceirizados para realizar serviços de revisão de registros é responsável por fornecer contexto sobre o ambiente da entidade aos prestadores de serviços, de modo que compreenda o ambiente da entidade, tenha uma linha de base de tráfego “normal” para a entidade e possa detectar possíveis problemas de segurança e fornecer exceções precisas e notificações de anomalias.
Requisitos da Abordagem Definida **10.4.1.1** Mecanismos automatizados são usados para realizar revisões de registro de auditoria. **Objetivo da Abordagem Personalizada** Atividades potencialmente suspeitas ou anômalas são identificadas por meio de um mecanismo consistente e repetível. **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.*	**Procedimentos de Teste da Abordagem Definida** **10.4.1.1** Examine os mecanismos de revisão de registro e entreviste o pessoal para verificar se os mecanismos automatizados são usados para realizar revisões de registro.	**Objetivo** As revisões manuais de registro são difíceis de realizar, mesmo para um ou dois sistemas, devido à quantidade de dados de registro que são gerados. No entanto, o uso de ferramentas de coleta, análise e alerta de registro, sistemas centralizados de gerenciamento de registro , analisadores de registro de eventos e sistemas de gerenciamento de eventos e informações de segurança (SIEM) podem ajudar a facilitar o processo, identificando eventos no registro que precisam ser revisados. **Práticas Recomendadas** A entidade deve manter as ferramentas de registro alinhadas com quaisquer alterações em seu ambiente, revisando periodicamente as configurações da ferramenta e atualizando as configurações para refletir quaisquer alterações.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **10.4.2** Os registros de todos os outros componentes de sistema (aqueles não especificados no Requisito 10.4.1) são revisados periodicamente.	**Procedimentos de Teste da Abordagem Definida** **10.4.2.a** Examine as políticas e procedimentos de segurança para verificar se os processos estão definidos para revisar os registros de todos os outros componentes de sistema periodicamente.	**Objetivo** A revisão periódica dos registros de todos os outros componentes de sistema (não especificados no Requisito 10.4.1) ajuda a identificar indicações de problemas potenciais ou tentativas de acessar sistemas críticos por meio de sistemas menos críticos.
	10.4.2.b Examine os resultados documentados das revisões do registro e entreviste o pessoal para verificar se as revisões do registro são realizadas periodicamente.	
Objetivo da Abordagem Personalizada Atividades potencialmente suspeitas ou anômalas para outros componentes de sistema (não incluídos em 10.4.1) são revisadas de acordo com o risco identificado da entidade.		
Observações de Aplicabilidade Este requisito é aplicável a todos os outros componentes de sistema dentro do escopo não incluídos no Requisito 10.4.1.		
Requisitos da Abordagem Definida **10.4.2.1** A frequência das revisões de registro periódicas para todos os outros componentes de sistema (não definidos no Requisito 10.4.1) é definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1	**Procedimentos de Teste da Abordagem Definida** **10.4.2.1.a** Examine a análise de risco direcionada da entidade para a frequência de revisões de registro periódicas para todos os outros componentes de sistema (não definidos no Requisito 10.4.1) para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1 .	**Objetivo** As entidades podem determinar o período ideal para revisar esses registros com base em critérios como a complexidade do ambiente de cada entidade, o número de tipos de sistemas que devem ser avaliados e as funções de tais sistemas.
	10.4.2.1.b Examine os resultados documentados das revisões periódicas do registro de todos os outros componentes de sistema (não definidos no Requisito 10.4.1) e entreviste o pessoal para *(continua na página a seguir)*	
Objetivo da Abordagem Personalizada As revisões de registro para componentes do sistema de baixo risco são realizadas com uma frequência que aborda o risco da entidade.		

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>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.</td><td>verificar se as revisões do registro são realizadas na frequência especificada na análise de risco direcionada da entidade realizada para este requisito.</td><td></td></tr>
<tr><td>Requisitos da Abordagem Definida

10.4.3 Exceções e anomalias identificadas durante o processo de revisão são tratadas.

Objetivo da Abordagem Personalizada

Atividades suspeitas ou anômalas são tratadas.</td><td>Procedimentos de Teste da Abordagem Definida

10.4.3.a Examine as políticas e procedimentos de segurança para verificar se os processos estão definidos para tratar as exceções e anomalias identificadas durante o processo de revisão.

10.4.3.b Observe os processos e entreviste o pessoal para verificar se, quando exceções e anomalias são identificadas, elas são tratadas.</td><td>Objetivo
Se as exceções e anomalias identificadas durante o processo de revisão de registro não forem investigadas, a entidade pode não estar ciente da ocorrência de atividades não autorizadas e potencialmente maliciosas em sua rede.
Práticas Recomendadas
As entidades deverão considerar como endereçar o seguinte ao desenvolver os seus processos para definir e administrar as exceções e as anomalias:
Como as atividades de revisão de registro são registradas,
Como classificar e priorizar exceções e anomalias,
Quais procedimentos devem ser implementados para relatar e escalar exceções e anomalias, e
Quem é responsável por investigar e por quaisquer tarefas de remediação.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
10.5 O histórico do registro de auditoria é retido e está disponível para análise.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Práticas Recomendadas** Reter registros de auditoria históricos por pelo menos 12 meses é necessário porque os comprometimentos muitas vezes passam despercebidos por períodos de tempo significativos. Ter o histórico do registro armazenado centralmente permite que os investigadores determinem melhor por quanto tempo uma violação potencial estava ocorrendo e o(s) sistema(s) possível(is) impactado(s). Por ter três meses de registros imediatamente disponíveis, uma entidade pode rapidamente identificar e minimizar o impacto de uma violação de dados **Exemplos** Os métodos que permitem que os registros estejam imediatamente disponíveis incluem o armazenamento de registros online, o arquivamento de registros ou a restauração rápida de registros de backups.
10.5.1 Reter o histórico do registro de auditoria por pelo menos 12 meses, com pelo menos os três meses mais recentes imediatamente disponíveis para análise.	**10.5.1.a** Examine a documentação para verificar se o seguinte está definido: • Políticas de retenção de registros de auditoria. • Procedimentos para reter o histórico do registro de auditoria por pelo menos 12 meses, com pelo menos os três meses mais recentes imediatamente disponíveis online.	
	10.5.1.b Examine as configurações do histórico do registro de auditoria, entreviste a equipe e examine-os para verificar se estes são retidos por pelo menos 12 meses.	
Objetivo da Abordagem Personalizada	**10.5.1.c** Entreviste a equipe e observe os processos para verificar se o histórico do registro de auditoria dos três meses mais recentes está imediatamente disponível para análise.	
Registros históricos de atividades estão disponíveis imediatamente para dar suporte à resposta a incidentes e são mantidos por pelo menos 12 meses.		

Requisitos e Procedimentos de Teste		Diretriz
10.6 Os mecanismos de sincronização de tempo suportam configurações de tempo consistentes em todos os sistemas.		
Requisitos da Abordagem Definida **10.6.1** Os relógios e a hora do sistema são sincronizados usando a tecnologia de sincronização de tempo. **Objetivo da Abordagem Personalizada** O tempo comum é estabelecido em todos os sistemas. **Observações de Aplicabilidade** Manter a tecnologia de sincronização de tempo atualizada inclui a gestão de vulnerabilidades, bem com aplicar patches na tecnologia de acordo com os Requisitos 6.3.1 e 6.3.3 do PCI DSS.	**Procedimentos de Teste da Abordagem Definida** **10.6.1** Examine as definições de configuração do sistema para verificar se a tecnologia de sincronização de tempo está implementada e mantida atualizada.	**Objetivo** A tecnologia de sincronização de tempo é usada para sincronizar relógios em vários sistemas. Quando os relógios não estão devidamente sincronizados, pode ser difícil, senão impossível, comparar arquivos de registro de sistemas diferentes e estabelecer uma sequência exata de eventos, o que é crucial para a análise forense após uma violação. Para equipes forenses pós-incidente, a precisão e consistência do tempo em todos os sistemas e o tempo de cada atividade são essenciais para determinar como os sistemas foram comprometidos. **Exemplos** O *Network Time Protocol* (NTP) é um exemplo de tecnologia de sincronização de tempo.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
10.6.2 Os sistemas são configurados para o tempo correto e consistente da seguinte forma: • Um ou mais servidores de tempo designados estão em uso. • Apenas o(s) servidor(es) de tempo central(is) designado(s) recebem 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 tempo designados aceitam atualizações de horário apenas de fontes externas específicas aceitas pela indústria. • Onde houver mais de um servidor de tempo designado, os servidores de tempo fazem par uns com os outros para manter o horário preciso. • Os sistemas internos recebem informações de horário apenas do(s) servidor(es) de tempo central(is) designado(s).	**10.6.2** Examine as definições de configuração do sistema para adquirir, distribuir e armazenar o tempo correto para verificar se as configurações estão definidas de acordo com todos os elementos especificados neste requisito.	O uso de servidores de tempo confiáveis é um componente crítico do processo de sincronização de tempo. Aceitar atualizações de horário de fontes externas específicas aceitas pela indústria ajuda a evitar que um indivíduo mal-intencionado altere as configurações de tempo nos sistemas. **Práticas Recomendadas** Outra opção para evitar o uso não autorizado de servidores de tempo internos é criptografar atualizações com uma chave simétrica e criar listas de controle de acesso que especificam os endereços IP de máquinas clientes que serão fornecidos com as atualizações de horário.
Objetivo da Abordagem Personalizada		
O tempo em todos os sistemas é precisa e consistente.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 alterações nas configurações de tempo em sistemas críticos são registradas, monitoradas e revisadas.	**10.6.3.a** Examine as configurações do sistema e as definições de sincronização de tempo para verificar se o acesso aos dados de tempo é restrito apenas ao pessoal com necessidades de negócio.	Os invasores tentarão alterar as configurações de tempo para ocultar sua atividade. Portanto, restringir a capacidade de alterar ou modificar as configurações de sincronização de horário ou o horário do sistema para os administradores diminuirá a probabilidade de um invasor alterar com êxito as configurações de tempo.
Objetivo da Abordagem Personalizada	**10.6.3.b** Examine as configurações do sistema e as configurações e registros de sincronização de tempo e observe os processos para verificar se todas as alterações nas configurações de tempo em sistemas críticos são registradas, monitoradas e revisadas.	
As configurações de tempo do sistema não podem ser modificadas por pessoal não autorizado.		

Requisitos e Procedimentos de Teste		Diretriz
10.7 Falhas de sistemas críticos de controle de segurança são detectadas, relatadas e respondidas prontamente.		
Requisitos da Abordagem Definida **10.7.1** ***Requisito adicional apenas para prestadores de serviços:*** Falhas de sistemas críticos de controle de segurança são detectadas, alertadas e resolvidas prontamente, incluindo, mas não se limitando a falha dos seguintes sistemas críticos de controle de segurança: • Controles de segurança de rede. • IDS/IPS. • FIM. • Soluções antimalware. • Controles de acesso físico. • Controles de acesso lógico. • Mecanismos de registro de auditoria. • Controles de segmentação (se usados). **Objetivo da Abordagem Personalizada** Falhas em sistemas críticos de controle de segurança são prontamente identificadas e tratadas. **Observações de Aplicabilidade** Este requisito se aplica apenas quando a entidade que está sendo avaliada é um prestador de serviços. Este requisito será substituído pelo Requisito 10.7.2 a partir de 31 de março de 2025.	**Procedimentos de Teste da Abordagem Definida** **10.7.1.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine a documentação para verificar se os processos estão definidos para a detecção e tratamento de falhas de sistemas críticos de controle de segurança realizadas prontamente, incluindo, mas não se limitando à falha de todos os elementos especificados neste requisito. **10.7.1.b Procedimentos de teste adicionais somente para as avaliações dos prestadores de serviço:** Observe os processos de detecção e alerta e entreviste o pessoal para verificar se as falhas dos sistemas críticos de controle de segurança são detectadas e relatadas e se a falha de um controle de segurança crítico resulta na geração de um alerta.	**Objetivo** Sem processos formais para detectar e alertar quando os controles de segurança críticos falham, as falhas podem passar despercebidas por longos períodos e fornecer aos invasores tempo suficiente para comprometer os componentes de sistema e roubar dados da conta do CDE. **Práticas Recomendadas** Os tipos específicos de falhas podem variar, dependendo da função do componente de sistema do dispositivo e da tecnologia em uso. Falhas típicas incluem um sistema que deixa de executar sua função de segurança ou não funciona da maneira pretendida, como um firewall apagando todas as suas regras ou ficando offline.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
10.7.2 Falhas de sistemas críticos de controle de segurança são detectadas, alertadas e tratadas prontamente, incluindo, mas não se limitando à falha dos seguintes sistemas críticos de controle de segurança: • 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).	**10.7.2.a** Examine a documentação para verificar se os processos estão definidos para a detecção e o tratamento de falhas de sistemas críticos de controle de segurança realizadas prontamente, incluindo, mas não se limitando à falha de todos os elementos especificados neste requisito.	Sem processos formais para detectar e alertar quando os controles de segurança críticos falham, as falhas podem passar despercebidas por longos períodos e fornecer aos invasores tempo suficiente para comprometer os componentes de sistema e roubar dados da conta do CDE. **Práticas Recomendadas** Os tipos específicos de falhas podem variar, dependendo da função do componente de sistema do dispositivo e da tecnologia em uso. No entanto, as falhas típicas incluem um sistema que não executa mais sua função de segurança ou não funciona da maneira pretendida - por exemplo, um firewall apagando suas regras ou ficando offline.
	10.7.2.b Observe os processos de detecção e alerta e entreviste o pessoal para verificar se as falhas dos sistemas críticos de controle de segurança são detectadas e relatadas e se a falha de um controle de segurança crítico resulta na geração de um alerta.	
Objetivo da Abordagem Personalizada		
Falhas em sistemas críticos de controle de segurança são prontamente identificadas e tratadas.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Este requisito se aplica a todas as entidades, incluindo os prestadores de serviço, e substituirá o Requisito 10.7.1 a partir de 31 de março de 2025. Inclui dois sistemas críticos de controle de segurança 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
10.7.3 Falhas de quaisquer sistemas críticos de controle de segurança são respondidas prontamente, incluindo, mas não se limitando a: • Restaurar as 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.	**10.7.3.a** Examine a documentação e entreviste o pessoal para verificar se os processos estão definidos e implementados para responder a uma falha de qualquer sistema crítico de controle de segurança e incluir pelo menos todos os elementos especificados neste requisito.	Se os alertas de falhas de sistemas críticos de controle de segurança não forem respondidos de forma rápida e eficaz, os invasores podem usar esse tempo para inserir software malicioso, obter o controle de um sistema ou roubar dados do ambiente da entidade. **Práticas Recomendadas** As evidências documentadas (por exemplo, registros em um sistema de gerenciamento de problemas) devem fornecer suporte de que os processos e procedimentos estão implementados para responder às falhas de segurança. Além disso, o pessoal deve estar ciente de suas responsabilidades em caso de falha. Ações e respostas à falha devem ser capturadas na evidência documentada.
Objetivo da Abordagem Personalizada	**10.7.3.b** Examine os registros para verificar se as falhas dos sistemas críticos de controle de segurança estão documentadas para incluir: • Identificação da(s) causa(s) da falha. • Duração (data e hora de início ao fim) da falha de segurança. • Detalhes da correção necessária para tratar a causa raiz.	
As falhas dos sistemas críticos de controle de segurança são analisadas, contidas e resolvidas, e os controles de segurança restaurados para minimizar o impacto. As questões de segurança resultantes são tratadas e medidas tomadas para prevenir a recorrência.		

(continua na página a seguir)

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
Este requisito aplica-se apenas quando a entidade a ser avaliada é um prestador 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. No entanto, 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

Seções	
11.1	Processos e mecanismos para testar regularmente a segurança de sistemas e redes são definidos e compreendidos.
11.2	Os pontos de acesso wireless são identificados e monitorados, e os pontos de acesso wireless não autorizados são endereçados.
11.3	Vulnerabilidades externas e internas são regularmente identificadas, priorizadas e tratadas.
11.4	Testes de penetração externos e internos são realizados regularmente e vulnerabilidades exploráveis e fragilidades de segurança são corrigidas.
11.5	Intrusões de rede e mudanças inesperadas de arquivos são detectadas e respondidas.
11.6	Mudanças não autorizadas nas páginas de pagamento são detectadas e respondidas.

Visão Geral

Vulnerabilidades estão sendo descobertas continuamente por indivíduos e pesquisadores mal-intencionados, e sendo introduzidas por novos softwares. Os componentes de sistema, processos e software sob medida e personalizados devem ser testados com frequência para garantir que os controles de segurança continuem a refletir um ambiente em mudança.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
11.1 Processos e mecanismos para testar regularmente a segurança de sistemas e redes são definidos e compreendidos.		
Requisitos da Abordagem Definida **11.1.1** Todas as políticas e processos operacionais identificados no Requisito 11 estão: • Documentados. • Atualizados. • Em uso. • De conhecimento de todas as partes afetadas. **Objetivo da Abordagem Personalizada** As expectativas, controles e supervisão para atendimento das atividades dentro do Requisito 11 são definidos e cumpridos pelo pessoal afetado. Todas as atividades de apoio são repetíveis, aplicadas de forma consistente e em conformidade com a intenção da gestão.	**Procedimentos de Teste da Abordagem Definida** **11.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** O Requisito 11.1.1 trata de gerenciar e manter com eficácia as várias políticas e procedimentos especificados em todo o Requisito 11. Embora seja importante definir as políticas ou procedimentos específicos mencionados no Requisito 11, é igualmente importante garantir que sejam devidamente documentados, mantidos e disseminados. **Práticas Recomendadas** É importante atualizar políticas e procedimentos conforme necessário para lidar com mudanças em processos, tecnologias e objetivos de negócios. Por esse motivo, considere atualizar esses documentos o mais rápido possível após a ocorrência de uma mudança e não apenas em um ciclo periódico. **Definições** As políticas de segurança definem os objetivos e princípios de segurança da entidade. Os procedimentos operacionais descrevem como realizar as atividades e definem os controles, métodos e processos que são seguidos para atingir o resultado desejado de maneira consistente e de acordo com os objetivos da política.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se as funções e responsabilidades não forem atribuídas formalmente, o pessoal pode não estar ciente de suas responsabilidades diárias e as atividades críticas podem não ocorrer. **Práticas Recomendadas** As funções e responsabilidades podem ser documentadas em políticas e procedimentos ou mantidas em documentos separados. Como parte da comunicação de funções e responsabilidades, as entidades podem considerar que o pessoal reconheça sua aceitação e compreensão de suas funções e responsabilidades atribuídas. **Exemplos** Um método para documentar funções e responsabilidades é uma matriz de atribuição de responsabilidades que inclui quem é responsável, responsabilizado, consultado e informado (também chamada de matriz RACI).
11.1.2 Funções e responsabilidades para a execução de atividades no Requisito 11 são documentados, atribuídos e compreendidos.	**11.1.2.a** Examine a documentação para verificar se as descrições de funções e responsabilidades para a execução de atividades no Requisito 11 estão documentadas e atribuídas.	
	11.1.2.b Entreviste a equipe responsável pela execução das atividades no Requisito 11 para verificar se as funções e responsabilidades são atribuídas conforme documentado e são compreendidas.	
Objetivo da Abordagem Personalizada		
As responsabilidades do dia a dia para realizar todas as atividades no Requisito 11 são alocadas. O pessoal é responsável pela operação contínua e bem-sucedida desses requisitos.		

Requisitos e Procedimentos de Teste		Diretriz
11.2 Os pontos de acesso wireless são identificados e monitorados, e os pontos de acesso wireless não autorizados são endereçados.		
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os pontos de acesso wireless não autorizados são identificados e endereçados periodicamente.	**Procedimentos de Teste da Abordagem Definida** **11.2.1.a** Examine as políticas e procedimentos para verificar se os processos são definidos para o gerenciamento de pontos de acesso wireless autorizados e não autorizados com todos os elementos especificados neste requisito. **11.2.1.b** Examine a(s) metodologia(s) em uso e a documentação resultante, e entreviste o pessoal para verificar se os processos estão definidos para detectar e identificar pontos de acesso wireless autorizados e não autorizados de acordo com todos os elementos especificados neste requisito. **11.2.1.c** Examine os resultados da avaliação wireless e entreviste o pessoal para verificar se as avaliações wireless foram conduzidas de acordo com todos os elementos especificados neste requisito. **11.2.1.d** Se o monitoramento automatizado for usado, examine as definições de configuração para verificar se a configuração irá gerar alertas para notificar o pessoal.	**Objetivo** A implementação e/ou exploração de tecnologia wireless em uma rede são caminhos comuns para usuários mal-intencionados obterem acesso não autorizado à rede e aos dados do titular do cartão. Dispositivos wireless não autorizados podem estar ocultos ou conectados a um computador ou outro componente de sistema. Esses dispositivos também podem ser conectados diretamente a uma porta de rede, a um dispositivo de rede, como um switch ou roteador, ou inseridos como uma placa de interface wireless dentro de um componente de sistema. Se um dispositivo ou rede wireless for instalado sem o conhecimento da empresa, ele pode permitir que um invasor entre na rede de forma fácil e “invisível”. Detectar e remover esses pontos de acesso não autorizados reduz a duração e a probabilidade de tais dispositivos serem aproveitados para um ataque. **Práticas Recomendadas** O tamanho e a complexidade de um ambiente ditarão as ferramentas e processos apropriados a serem usados para fornecer garantia suficiente de que um ponto de acesso wireless não autorizado não foi instalado no ambiente. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade O requisito se aplica mesmo quando existe uma política que proíbe o uso de tecnologia wireless, uma vez que os invasores não leem e não seguem a política da empresa. 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.		Por exemplo, realizar uma inspeção física detalhada de um único quiosque de varejo autônomo em um shopping center, onde todos os componentes de comunicação estão contidos em invólucros resistentes a modificação e cuja modificação seja evidente pode ser suficiente para fornecer a garantia de que um ponto de acesso wireless não autorizado não foi anexado ou instalado. No entanto, em um ambiente com vários nós (como em uma grande loja de varejo, call center, sala de servidores ou data center), a inspeção física detalhada pode ser difícil. Nesse caso, vários métodos podem ser combinados, como a realização de inspeções físicas do sistema em conjunto com os resultados de um analisador wireless. **Definições** Isso também é conhecido como detecção de ponto de acesso não autorizado. **Exemplos** Os métodos que podem ser usados incluem, mas não estão limitados a varreduras de rede wireless, inspeções físicas/lógicas de componentes de sistema e infraestrutura, controle de acesso à rede (NAC) ou IDS/IPS wireless. NAC e IDS/IPS wireless são exemplos de ferramentas de monitoramento automatizadas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **11.2.2** Um inventário de pontos de acesso wireless autorizados é mantido, incluindo uma justificativa de negócio documentada. **Objetivo da Abordagem Personalizada** Pontos de acesso wireless não autorizados não são confundidos com pontos de acesso wireless autorizados.	**Procedimentos de Teste da Abordagem Definida** **11.2.2** Examine a documentação para verificar se um inventário de pontos de acesso wireless autorizados é mantido e uma justificativa de negócios é documentada para todos os pontos de acesso wireless autorizados.	**Objetivo** Um inventário de pontos de acesso wireless autorizados pode ajudar os administradores a responder rapidamente quando pontos de acesso wireless não autorizados são detectados. Isso ajuda a minimizar proativamente a exposição do CDE a indivíduos mal-intencionados. **Práticas Recomendadas** Se estiver usando um scanner wireless, é igualmente importante ter uma lista definida de pontos de acesso conhecidos que, embora não estejam conectados à rede da empresa, geralmente serão detectados durante uma varredura. Esses dispositivos que não pertencentes à empresa costumam ser encontrados em edifícios ou empresas multilocatárias localizadas próximas umas das outras. No entanto, é importante verificar se esses dispositivos não estão conectados à porta de rede da entidade ou por meio de outro dispositivo conectado à rede e recebem um SSID semelhante a uma empresa próxima. Os resultados da varredura devem observar tais dispositivos e como foi determinado que esses dispositivos poderiam ser "ignorados". Além disso, a detecção de quaisquer pontos de acesso wireless não autorizados que sejam considerados uma ameaça ao CDE deve ser gerenciada de acordo com o plano de resposta a incidentes da entidade de acordo com o Requisito 12.10.1.

Requisitos e Procedimentos de Teste		Diretriz
11.3 Vulnerabilidades externas e internas são regularmente identificadas, priorizadas e tratadas.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
11.3.1 As varreduras de vulnerabilidade interna são realizadas da seguinte forma: • Pelo menos uma vez a cada três meses. • Vulnerabilidades de alto risco e críticas (de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) são resolvidas. • "Rescans [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.	**11.3.1.a** Examine os resultados do relatório de varredura interna dos últimos 12 meses para verificar se as varreduras internas ocorreram pelo menos uma vez a cada três meses nos últimos 12 meses **11.3.1.b** Examine os resultados do relatório de varredura interna de cada varredura e nova varredura nos últimos 12 meses para verificar se todas as vulnerabilidades críticas e de alto risco (identificadas no Requisito 6.3.1 do PCI DSS) foram resolvidas. **11.3.1.c** Examine as configurações da ferramenta de varredura e entreviste a equipe para verificar se a ferramenta de varredura é mantida atualizada com as informações mais recentes sobre vulnerabilidades. **11.3.1.d** Entreviste a equipe responsável para verificar se a varredura foi realizada por recurso(s) interno(s) qualificado(s) ou terceiro externo qualificado e se existe independência organizacional do testador.	**Objetivo** Identificar e resolver vulnerabilidades reduz prontamente a probabilidade de uma vulnerabilidade ser explorada e o comprometimento potencial de um componente de sistema ou dos dados do titular do cartão. Varreduras de vulnerabilidade conduzidas pelo menos a cada três meses fornecem essa detecção e identificação. **Práticas Recomendadas** Vulnerabilidades que representam o maior risco para o ambiente (por exemplo, classificação alta ou crítica de acordo com o Requisito 6.3.1) devem ser resolvidas com a mais alta prioridade. Vários relatórios de varredura podem ser combinados para o processo de varredura trimestral para mostrar que todos os sistemas foram varridos e todas as vulnerabilidades aplicáveis foram resolvidas como parte do ciclo de varredura de vulnerabilidade de três meses. No entanto, pode ser necessária documentação adicional para verificar se as vulnerabilidades não corrigidas estão em processo de resolução. Embora as varreduras sejam necessárias pelo menos uma vez a cada três meses, varreduras mais frequentes são recomendadas, dependendo da complexidade da rede, frequência de mudanças e tipos de dispositivos, software e sistemas operacionais usados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada A postura de segurança de todos os componentes de sistema é verificada periodicamente usando ferramentas automatizadas projetadas para detectar vulnerabilidades operando dentro da rede. As vulnerabilidades detectadas são avaliadas e retificadas com base em uma estrutura formal de avaliação de risco. **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) de 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 varreduras de vulnerabilidade interna realizadas por uma empresa especializada em varredura de vulnerabilidades.		**Definições** Uma varredura de vulnerabilidade é uma combinação de ferramentas, técnicas e/ou métodos automatizados executados contra dispositivos e servidores externos e internos, projetados para expor vulnerabilidades potenciais em aplicativos, sistemas operacionais e dispositivos de rede que podem ser encontrados e explorados por indivíduos mal-intencionados.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
11.3.1.1 Todas as outras vulnerabilidades aplicáveis (aquelas não classificadas como 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: • Tratadas com base no risco definido na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1. • "Rescans [novas varreduras]" são realizadas conforme necessário.	**11.3.1.1.a** Examine a análise de risco direcionada da entidade que define o risco para tratar todas as outras vulnerabilidades aplicáveis (aquelas não classificadas como de alto risco ou críticas pelas classificações de risco de vulnerabilidade da entidade no Requisito 6.3.1) para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1.	Todas as vulnerabilidades, independentemente da gravidade, fornecem uma via potencial de ataque e, portanto, devem ser tratadas periodicamente, com as vulnerabilidades que expõem o maior risco abordadas mais rapidamente para limitar a janela potencial de ataque.
Objetivo da Abordagem Personalizada	**11.3.1.1.b** Entreviste a equipe responsável e examine os resultados do relatório de varredura interna ou outra documentação para verificar se todas as outras vulnerabilidades aplicáveis (aquelas não classificadas como de alto risco ou críticas pelas classificações de risco de vulnerabilidade da entidade no Requisito 6.3.1) são tratadas com base em o risco definido na análise de risco direcionada da entidade e que o processo de varredura inclui novas varreduras, conforme necessário, para confirmar se as vulnerabilidades foram resolvidas.	
Vulnerabilidades com classificação inferior (inferior a alta ou crítica) são tratadas com uma frequência de acordo com o risco da entidade.		
Observações de Aplicabilidade		
O prazo para tratar 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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. • São usados privilégios suficientes, 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.	**11.3.1.2.a** Examine as configurações da ferramenta de varredura para verificar se a varredura autenticada é usada para varreduras internas, com privilégios suficientes, para os sistemas que aceitam credenciais para varredura.	A varredura autenticada fornece uma visão melhor do cenário de vulnerabilidade de uma entidade, uma vez que pode detectar vulnerabilidades que as varreduras não autenticadas não podem detectar. Os invasores podem aproveitar vulnerabilidades das quais uma entidade não tem conhecimento porque certas vulnerabilidades só serão detectadas com varredura autenticada. A varredura autenticada pode gerar informações adicionais significativas sobre as vulnerabilidades de uma organização. **Práticas Recomendadas** As credenciais usadas para essas varreduras devem ser consideradas altamente privilegiadas. Elas devem ser protegidas e controladas como tal, de acordo com os Requisitos 7 e 8 do PCI DSS (exceto para aqueles requisitos para autenticação multifator e contas de aplicativo e sistema).
	11.3.1.2.b Examine os resultados do relatório de varredura e entreviste a equipe para verificar se as varreduras autenticadas são realizadas.	
Objetivo da Abordagem Personalizada Ferramentas automatizadas usadas para detectar vulnerabilidades podem detectar vulnerabilidades locais para cada sistema, que não são visíveis remotamente.	**11.3.1.2.c** Se as contas usadas para varredura autenticada puderem ser usadas para login interativo, examine as contas e entreviste a equipe para verificar se as contas são gerenciadas de acordo com todos os elementos especificados no Requisito 8.2.2.	
	11.3.1.2.d Examine a documentação para verificar se os sistemas que não podem aceitar credenciais para verificação autenticada estão definidos.	

(continua na página a seguir)

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade		
As ferramentas de varredura 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 de 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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A varredura de um ambiente após quaisquer mudanças significativas garante que as mudanças foram concluídas de forma adequada, de forma que a segurança do ambiente não foi comprometida por causa da mudança. **Práticas Recomendadas** As entidades devem realizar varreduras após mudanças significativas como parte do processo de mudança de acordo com o Requisito 6.5.2 e antes de considerar a mudança concluída. Todos os componentes de sistema afetados pela mudança precisarão ser verificados.
11.3.1.3 Varreduras de vulnerabilidades internas são realizadas após qualquer mudança significativa da seguinte forma: • Vulnerabilidades de alto risco e críticas (de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) são resolvidas. • "Rescans [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).	**11.3.1.3.a** Examine a documentação de controle de mudanças e os relatórios de varredura interna para verificar se os componentes de sistema foram varridos após qualquer mudança significativa.	
	11.3.1.3.b Entreviste a equipe e examine os relatórios de varredura interna e novas varreduras para verificar se as varreduras internas foram realizadas após mudanças significativas e se as vulnerabilidades críticas e de alto risco, conforme definidas no Requisito 6.3.1, foram resolvidas.	
Objetivo da Abordagem Personalizada A postura de segurança de todos os componentes de sistema é verificada após mudanças significativas na rede ou sistemas, usando ferramentas automatizadas projetadas para detectar vulnerabilidades operando dentro da rede. As vulnerabilidades detectadas são avaliadas e retificadas com base em uma estrutura formal de avaliação de risco	**11.3.1.3.c** Entreviste a equipe para verificar se as varreduras internas são realizadas por recursos internos qualificados ou terceiros externos qualificados e se existe independência organizacional do testador.	
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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
11.3.2 As varreduras de vulnerabilidade externa são realizadas da seguinte forma: • Pelo menos uma vez a cada três meses. • Por Fornecedor de Varredura Aprovado do PCI SSC (ASV). • As vulnerabilidades foram resolvidas e os requisitos do Guia do Programa ASV para uma varredura aprovada 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 aprovada.	**11.3.2.a** Examine os relatórios de varredura ASV dos últimos 12 meses para verificar se as varreduras externas de vulnerabilidade ocorreram pelo menos uma vez a cada três meses nos últimos 12 meses. **11.3.2.b** Examine o relatório de varredura ASV de cada varredura e de nova varredura nos últimos 12 meses para verificar se as vulnerabilidades foram resolvidas e se os requisitos do Guia do Programa ASV para uma varredura aprovada foram atendidos. **11.3.2.c** Examine os relatórios de varredura ASV para verificar se as varreduras foram concluídas por um Fornecedor de Varredura aprovado (ASV) do PCI SSC.	Os invasores procuram rotineiramente por servidores externos não corrigidos ou vulneráveis, que podem ser aproveitados para lançar um ataque direcionado. As organizações devem garantir que esses dispositivos externos sejam verificados regularmente em busca de pontos fracos e que as vulnerabilidades sejam corrigidas ou remediadas para proteger a entidade. Como as redes externas correm maior risco de comprometimento, a varredura de vulnerabilidade externa deve ser realizada pelo menos uma vez a cada três meses por um Fornecedor de Varredura Aprovado (ASV) do PCI SSC. **Práticas Recomendadas** Embora as varreduras sejam necessárias pelo menos uma vez a cada três meses, varreduras mais frequentes são recomendadas, dependendo da complexidade da rede, frequência de mudanças e tipos de dispositivos, software e sistemas operacionais usados. Vários relatórios de varredura podem ser combinados para mostrar que todos os sistemas foram varridos e que todas as vulnerabilidades aplicáveis foram resolvidas como parte do ciclo de varredura de vulnerabilidade de três meses. No entanto, pode ser necessária documentação adicional para verificar se as vulnerabilidades não corrigidas estão em processo de resolução.
Objetivo da Abordagem Personalizada Este requisito não se aplica às abordagens personalizadas.		
Observações de Aplicabilidade Para conformidade inicial com o PCI DSS, 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 aprovada, 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). *(continua na página a seguir)*		

Requisitos e Procedimentos de Teste		Diretriz
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 na 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A varredura de um ambiente após quaisquer mudanças significativas garante que as mudanças foram concluídas de forma adequada, de forma que a segurança do ambiente não foi comprometida por causa da mudança. **Práticas Recomendadas** As entidades devem incluir a necessidade de realizar varreduras após mudanças significativas como parte do processo de mudança e antes que a mudança seja considerada concluída. Todos os componentes de sistema afetados pela mudança precisarão ser verificados.
11.3.2.1 Varreduras de vulnerabilidades internas são realizadas após qualquer mudança significativa da seguinte forma: Vulnerabilidades com pontuação de 4.0 ou superior pelo CVSS são resolvidas. “Rescans [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).	**11.3.2.1.a** Examine a documentação de controle de mudanças e os relatórios de varredura externa para verificar se os componentes de sistema foram varridos após qualquer mudança significativa.	
	11.3.2.1.b Entreviste a equipe e examine os relatórios de varredura externa e novas varreduras para verificar se as varreduras externas foram realizadas após mudanças significativas e se as vulnerabilidades com classificação 4.0 ou superior pelo CVSS foram resolvidas.	
Objetivo da Abordagem Personalizada	**11.3.2.1.c** Entreviste a equipe para verificar se as varreduras externas são realizadas por recursos internos qualificados ou terceiros externos qualificados e se existe independência organizacional do testador.	
A postura de segurança de todos os componentes de sistema é verificada após mudanças significativas na rede ou sistemas, usando ferramentas projetadas para detectar vulnerabilidades operando de fora da rede. As vulnerabilidades detectadas são avaliadas e retificadas com base em uma estrutura formal de avaliação de risco		

Requisitos e Procedimentos de Teste		Diretriz
11.4 Testes de penetração externos e internos são realizados regularmente e vulnerabilidades exploráveis e fragilidades de segurança são corrigidas.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Os atacantes gastam muito tempo encontrando vulnerabilidades externas e internas para a seu aprimoramento a fim de obter acesso aos dados do titular do cartão e, em seguida, exfiltrar esses dados. Como tal, as entidades precisam testar suas redes completamente, assim como um atacante faria. Este teste permite que a entidade identifique e corrija a fraqueza que pode ser aproveitada para comprometer a rede e os dados da entidade e, em seguida, tomar as ações apropriadas para proteger a rede e os componentes de sistema de tais ataques. **Práticas Recomendadas** As técnicas de teste de penetração serão diferentes com base nas necessidades e estrutura de uma organização e devem ser adequadas para o ambiente testado - por exemplo, testes de *fuzzing*, injeção e falsificação podem ser apropriados. O tipo, a profundidade e a complexidade do teste dependerão do ambiente específico e das necessidades da organização. **Definições** Os testes de penetração simulam uma situação de ataque do mundo real com a intenção de identificar o quanto um atacante pode penetrar em um ambiente, dadas diferentes quantidades de informações fornecidas ao testador. Isso permite que uma entidade entenda melhor sua exposição potencial e desenvolva uma estratégia de defesa contra ataques. Um teste de penetração difere de uma varredura de vulnerabilidade, pois um teste de penetração é um processo ativo que geralmente inclui a exploração de vulnerabilidades identificadas. *(continua na página a seguir)*
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 do CDE e sistemas críticos. • Teste 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.	**11.4.1** Examine a documentação e entreviste o pessoal para verificar se a metodologia de teste de penetração definida, documentada e implementada pela entidade inclui todos os elementos especificados neste requisito.	

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Uma metodologia formal é definida para testes técnicos completos que tentam explorar vulnerabilidades e fraquezas de segurança por meio de métodos de ataque simulado por um atacante manual competente.		A varredura de vulnerabilidades por si só não é um teste de penetração, nem é um teste de penetração adequado se o foco for unicamente tentar explorar vulnerabilidades encontradas em uma varredura de vulnerabilidade. A realização de uma varredura de vulnerabilidade pode ser uma das primeiras etapas, mas não é a única etapa que um testador de penetração realizará para planejar a estratégia de teste. Mesmo que uma varredura de vulnerabilidade não detecte vulnerabilidades conhecidas, o testador de penetração geralmente obterá conhecimento suficiente sobre o sistema para identificar possíveis falhas de segurança. O teste de penetração é um processo altamente manual. Embora algumas ferramentas automatizadas possam ser usadas, o testador usa seu conhecimento de sistemas para obter acesso a um ambiente. Frequentemente, o testador irá encadear vários tipos de explorações com o objetivo de romper camadas de defesas. Por exemplo, se o testador encontrar uma maneira de obter acesso a um servidor de aplicativos, ele usará o servidor comprometido como um ponto para preparar um novo ataque com base nos recursos aos quais o servidor tem acesso. Dessa forma, um testador pode simular as técnicas usadas por um invasor para identificar áreas de fraqueza potencial no ambiente. O teste dos métodos de monitoramento de segurança e de detecção - por exemplo, para confirmar a eficácia dos mecanismos de monitoramento de registro e integridade de arquivo, também deve ser considerado. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Testar de dentro da rede (ou "teste de penetração interno") significa testar de dentro do CDE e no CDE desde 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.		**Informações Adicionais** Consulte *Information Supplement: Penetration Testing Guidance* para diretrizes adicionais. As abordagens de teste de penetração aceitas pela indústria incluem: *The Open Source Security Testing Methodology and Manual (OSSTMM)* *Programas de Teste de Penetração do Open Web Application Security Project (OWASP).*
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 atualização ou mudança significativa da infraestrutura ou 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).	**11.4.2.a** Examine o escopo do trabalho e os resultados do teste de penetração interna mais recente para verificar se o teste de penetração é executado de acordo com todos os elementos especificados neste requisito. **11.4.2.b** Entreviste a equipe para verificar se o teste de penetração interno foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e se existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	O teste de penetração interna tem dois propósitos. Em primeiro lugar, assim como um teste de penetração externo, ele descobre vulnerabilidades e configurações incorretas que podem ser usadas por um atacante que conseguiu obter algum grau de acesso à rede interna, seja porque o atacante é um usuário autorizado conduzindo atividades não autorizadas, ou um atacante externo que conseguiu penetrar no perímetro da entidade. Em segundo lugar, o teste de penetração interno também ajuda as entidades a descobrir onde seu processo de controle de mudanças falhou, detectando sistemas anteriormente desconhecidos. Além disso, verifica o status de muitos dos controles que operam no CDE. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada As defesas internas do sistema são verificadas por testes técnicos de acordo com a metodologia definida pela entidade com a frequência necessária para lidar com a evolução e novos ataques e ameaças e garantir que mudanças significativas não introduzam vulnerabilidades desconhecidas.		Um teste de penetração não é verdadeiramente um "teste" porque o resultado de um teste de penetração não é algo que pode ser classificado como "aprovado" ou "reprovado". O melhor resultado de um teste é um catálogo de vulnerabilidades e configurações incorretas que uma entidade não conhecia e que o testador de penetração as encontrou antes que um atacante. Um teste de penetração que não encontrou nada é tipicamente indicativo de deficiências do testador de penetração, em vez de ser um reflexo positivo da postura de segurança da entidade. **Práticas Recomendadas** Algumas considerações ao escolher um recurso qualificado para realizar o teste de penetração incluem: • Certificações específicas de testes de penetração, que podem ser uma indicação do nível de habilidade e competência do testador. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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 atualização ou mudança significativa da infraestrutura ou 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).	**11.4.3.a** Examine o escopo do trabalho e os resultados do teste de penetração externa mais recente para verificar se o teste de penetração é executado de acordo com todos os elementos especificados neste requisito.	• Experiência anterior na realização de testes de penetração - por exemplo, o número de anos de experiência e o tipo e escopo de trabalhos anteriores pode ajudar a confirmar se a experiência do testador é apropriada para as necessidades do trabalho. **Informações Adicionais** Consulte *Information Supplement: Penetration Testing Guidance* no site do PCI SSC para orientações adicionais.
	11.4.3.b Entreviste o pessoal para verificar se o teste de penetração externa foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e se existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	
Objetivo da Abordagem Personalizada		
As defesas externas do sistema são verificadas por testes técnicos de acordo com a metodologia definida pela entidade, com a frequência necessária para lidar com a evolução e novos ataques e ameaças, e para garantir que mudanças significativas não introduzam vulnerabilidades desconhecidas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 sobre o risco representado pelo problema de segurança, conforme definido no Requisito 6.3.1. • O teste de penetração é repetido para verificar as correções.	**11.4.4** Examine os resultados do teste de penetração para verificar se as vulnerabilidades exploráveis e os pontos fracos de segurança foram corrigidos de acordo com todos os elementos especificados neste requisito.	Os resultados de um teste de penetração são geralmente uma lista priorizada de vulnerabilidades descobertas pelo exercício. Frequentemente, um testador terá encadeado uma série de vulnerabilidades para comprometer um componente de sistema. A correção das vulnerabilidades encontradas por um teste de penetração reduz significativamente a probabilidade de que as mesmas vulnerabilidades sejam exploradas por um atacante mal-intencionado. Usar o próprio processo de avaliação de risco de vulnerabilidade da entidade (consulte o requisito 6.3.1) garante que as vulnerabilidades que representam o maior risco para a entidade sejam corrigidas mais rapidamente
Objetivo da Abordagem Personalizada		**Práticas Recomendadas**
Vulnerabilidades e fragilidades de segurança encontradas durante a verificação das defesas do sistema são mitigadas.		Como parte da avaliação de risco da entidade, as entidades devem considerar a probabilidade de a vulnerabilidade ser explorada e se existem outros controles presentes no ambiente para reduzir o risco. Quaisquer deficiências que apontam para os requisitos do PCI DSS não sendo atendidos devem ser tratadas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 mudanças 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. • Confirmando se os controles/métodos de segmentação são operacionais e eficazes, e isolam o CDE de todos os sistemas fora do escopo. • Confirmando a 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).	**11.4.5.a** Examine os controles de segmentação e Examine a metodologia de teste de penetração para verificar se os procedimentos de teste de penetração estão definidos para testar todos os métodos de segmentação de acordo com todos os elementos especificados neste requisito. **11.4.5.b** Examine os resultados do teste de penetração mais recente para verificar se o teste de penetração cobre e aborda todos os elementos especificados neste requisito. **11.4.5.c** Entreviste a equipe para verificar se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e se existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	Quando uma entidade usa controles de segmentação para isolar o CDE de redes internas não confiáveis, a segurança do CDE depende do funcionamento da segmentação. Muitos ataques envolveram o atacante movendo-se lateralmente no que uma entidade considerou uma rede isolada para o CDE. O uso de ferramentas e técnicas de teste de penetração para validar se uma rede não confiável está realmente isolada do CDE pode alertar a entidade sobre uma falha ou configuração incorreta dos controles de segmentação, que podem então ser retificados. **Práticas Recomendadas** Técnicas como descoberta de host e varredura de porta podem ser usadas para verificar se os segmentos fora do escopo não têm acesso ao CDE.
Objetivo da Abordagem Personalizada		
Se a segmentação for usada, ela é verificada periodicamente por testes técnicos para ser continuamente eficaz, incluindo após quaisquer mudanças, no isolamento do CDE de todos os sistemas fora do escopo.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
11.4.6 ***Requisito adicional apenas para prestadores de serviços:*** 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 seis meses e após quaisquer mudanças 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. • Confirmando se os controles/métodos de segmentação são operacionais e eficazes e isolar o CDE de todos os sistemas fora do escopo. • Confirmando a 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).	**11.4.6.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine os resultados do teste de penetração mais recente para verificar se o teste de penetração cobre e aborda todos os elementos especificados neste requisito. **11.4.6.b** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Entreviste a equipe para verificar se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e se existe independência organizacional do testador (não é necessário ser um QSA ou ASV).	Os prestadores de serviço normalmente têm acesso a grandes volumes de dados do titular do cartão ou podem fornecer um ponto de entrada que pode ser explorado para comprometer várias outras entidades. Os prestadores de serviços também costumam ter redes maiores e mais complexas, sujeitas a mudanças mais frequentes. A probabilidade de falha nos controles de segmentação em redes complexas e dinâmicas é maior em ambientes de prestadores de serviços. Validar os controles de segmentação com mais frequência provavelmente descobrirá essas falhas antes que elas possam ser exploradas por um atacante que tenta mover lateralmente de uma rede não confiável fora do escopo para o CDE. **Práticas Recomendadas** Embora o requisito especifique que essa validação de escopo seja realizada pelo menos uma vez a cada seis meses e após uma mudança significativa, este exercício deve ser realizado com a maior frequência possível para garantir que permaneça eficaz no isolamento do CDE de outras redes.
Objetivo da Abordagem Personalizada		
Se a segmentação for usada, ela é verificada por testes técnicos para ser continuamente eficaz, incluindo após quaisquer mudanças, no isolamento do CDE dos sistemas fora do escopo. *(continua na página a seguir)*		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		
Requisitos da Abordagem Definida **11.4.7** ***Requisito adicional apenas para prestadores de serviços multilocatários:*** Os prestadores de serviços em nuvem/hospedados por terceiros oferecem suporte a seus clientes para testes de penetração externa de acordo com os Requisitos 11.4.3 e 11.4.4. **Objetivo da Abordagem Personalizada** Prestadores de serviços multilocatários dão suporte à necessidade de seus clientes por testes técnicos, fornecendo acesso ou evidência de que testes técnicos comparáveis foram realizados. **Observações de Aplicabilidade** Este requisito se aplica somente quando a entidade que está sendo avaliada é um prestador de serviços multilocatário. Para atender a esse requisito, os prestadores de serviços multilocatários podem: • Fornecer evidências aos seus clientes para mostrar que o teste de penetração foi realizado de acordo com os Requisitos 11.4.3 e 11.4.4 na infraestrutura assinada pelos clientes, ou • Fornecer acesso imediato a cada um de seus clientes, para que eles possam realizar seus próprios testes de penetração. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **11.4.7** ***Procedimentos de teste adicionais apenas para prestadores de serviços multilocatários:*** Examine as evidências para verificar se os prestadores de multilocatário oferecem suporte a seus clientes para testes de penetração externa de acordo com os Requisitos 11.4.3 e 11.4.4.	**Objetivo** As entidades precisam realizar testes de penetração de acordo com o PCI DSS para simular o comportamento do invasor e descobrir vulnerabilidades em seu ambiente. Em ambientes compartilhados e em nuvem, o prestador de serviços multilocatários pode estar preocupado com as atividades de um testador de penetração afetando os sistemas de outros clientes Os Prestadores de Serviço Multilocatário não podem proibir o teste de penetração porque isso deixaria os sistemas de seus clientes abertos à exploração. Portanto, os prestadores de serviços multilocatário devem oferecer suporte às solicitações do cliente para realizar testes de penetração ou para resultados de testes de penetração.

Requisitos e Procedimentos de Teste		Diretriz
As evidências fornecidas aos clientes podem incluir resultados de testes de penetração editados, mas precisam incluir informações suficientes para provar que todos os elementos dos Requisitos 11.4.3 e 11.4.4 foram atendidos em nome do cliente. Consulte também o Apêndice A1: Requisitos Adicionais do PCI DSS para Prestadores de Serviço Multilocatários. *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.*		

Requisitos e Procedimentos de Teste		Diretriz
11.5 Intrusões de rede e mudanças inesperadas de arquivos são detectadas e respondidas.		
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Mecanismos para detectar tráfego de rede suspeito ou anômalo em tempo real que podem ser indicativos de atividade de ator de ameaça são implementados. Os alertas gerados por esses mecanismos são respondidos pelo pessoal ou por meios automatizados que garantem que os componentes de sistema não sejam comprometidos como resultado da atividade detectada.	**Procedimentos de Teste da Abordagem Definida** **11.5.1.a** Examine as configurações do sistema e diagramas de rede para verificar se as técnicas de detecção de intrusão e/ou prevenção de intrusão estão implementadas para monitorar todo o tráfego: • No perímetro do CDE. • Em pontos críticos do CDE. **11.5.1.b** Examine as configurações do sistema e entreviste o pessoal responsável para verificar a detecção de intrusão e/ou as técnicas de prevenção de intrusão alertam o pessoal de comprometimentos suspeitos. **11.5.1.c** Examine as configurações do sistema e a documentação do fornecedor para verificar se as técnicas de detecção de intrusão e/ou prevenção de intrusão estão configuradas para manter todos os mecanismos, linhas de base e assinaturas atualizados.	**Objetivo** As técnicas de detecção de intrusão e/ou prevenção de intrusão (como IDS/IPS) comparam o tráfego que entra na rede com "assinaturas" conhecidas e/ou comportamentos de milhares de tipos de comprometimento (ferramentas de hacker, cavalos de Troia e outros malwares) e em seguida, envia alertas e/ou interrompem a tentativa conforme ela acontece. Sem uma abordagem proativa para detectar atividades não autorizadas, os ataques (ou uso indevido) dos recursos do computador podem passar despercebidos por longos períodos de tempo. O impacto de uma intrusão no CDE é, em muitos aspectos, um fator do tempo que um invasor tem no ambiente antes de ser detectado. **Práticas Recomendadas** Os alertas de segurança gerados por essas técnicas devem ser monitorados continuamente, de modo que as tentativas ou intrusões reais possam ser interrompidas e os danos potenciais limitados. **Definições** Locais críticos podem incluir, mas não estão limitados a, controles de segurança de rede entre segmentos de rede (por exemplo, entre uma DMZ e uma rede interna ou entre uma rede dentro e fora do escopo) e pontos que protegem as conexões entre uma rede menos confiável e um componente de sistema mais confiável.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
11.5.1.1 ***Requisito adicional apenas para prestadores de serviços:*** As técnicas de detecção de intrusão e/ou prevenção de intrusão detectam, alertam/previnem e abordam canais de comunicação de malware ocultos.	**11.5.1.1.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine a documentação e as definições de configuração para verificar se os métodos para detectar e alertar/prevenir canais de comunicação secretos de malware estão disponíveis e operando.	**Objetivo** A detecção de tentativas de comunicação secretas de malware (por exemplo, túnel DNS) pode ajudar a bloquear a disseminação de malware lateralmente dentro de uma rede e a exfiltração de dados. Ao decidir onde colocar esse controle, as entidades devem considerar locais críticos na rede e prováveis rotas para canais secretos. Quando o malware se estabelece em um ambiente infectado, geralmente tenta estabelecer um canal de comunicação com um servidor de comando e controle (C&C). Por meio do servidor C&C, o invasor se comunica e controla o malware em sistemas comprometidos para entregar cargas ou instruções maliciosas ou para iniciar a exfiltração de dados. Em muitos casos, o malware se comunicará com o servidor C&C indiretamente por meio de botnets, ignorando o monitoramento, bloqueando controles e tornando esses métodos ineficazes para detectar os canais secretos. **Práticas Recomendadas** Os métodos que podem ajudar a detectar e abordar os canais de comunicação de malware incluem varredura de endpoint em tempo real, filtragem de tráfego de saída, uma lista de "permissões", ferramentas de prevenção de perda de dados e ferramentas de monitoramento de segurança de rede, como IDS/IPS. Além disso, as consultas e respostas do DNS são uma fonte de dados chave usada pelos defensores da rede para apoiar a resposta a incidentes e também a descoberta de intrusões. *(continua na página a seguir)*
	11.5.1.1.b ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine o plano de resposta a incidentes da entidade (Requisito 12.10.1) para verificar se ele exige e define uma resposta no caso de canais ocultos de comunicação de malware serem detectados.	
Objetivo da Abordagem Personalizada	**11.5.1.1.c** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Entreviste a equipe responsável e observe os processos para verificar se a equipe mantém conhecimento da comunicação oculta de malware e das técnicas de controle e sabe como responder quando há suspeita de malware.	
Existem mecanismos para detectar e alertar/prevenir comunicações secretas com sistemas de comando e controle. Os alertas gerados por esses mecanismos são respondidos pelo pessoal ou por meios automatizados que garantem o bloqueio dessas comunicações.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. *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.*		Quando essas transações são coletadas para processamento e análise, elas podem permitir uma série de cenários analíticos de segurança valiosos. É importante que as organizações mantenham um conhecimento atualizado dos modos de operação do malware, pois atenuá-los pode ajudar a detectar e limitar o impacto do malware no ambiente.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 alterações, adições e exclusões) de arquivos críticos. • Para realizar comparações críticas de arquivos pelo menos uma vez por semana.	**11.5.2.a** Examine as configurações do sistema, os arquivos monitorados e os resultados das atividades de monitoramento para verificar o uso de um mecanismo de detecção de mudanças.	Mudanças em arquivos críticos de sistema, configuração ou conteúdo podem ser um indicador de que um atacante acessou o sistema de uma organização. Essas alterações podem permitir que um atacante execute ações maliciosas adicionais, acesse os dados do titular do cartão e/ou conduza atividades sem detecção ou registro. Um mecanismo de detecção de mudanças detectará e avaliará essas mudanças em arquivos críticos e gerará alertas que podem ser respondidos de acordo com processos definidos para que o pessoal possa tomar as ações apropriadas. Se não for implementado corretamente e a saída da solução de detecção de mudanças monitorada, um indivíduo mal-intencionado pode adicionar, remover ou alterar o conteúdo do arquivo de configuração, programas do sistema operacional ou executáveis do aplicativo. Mudanças não autorizadas, se não detectadas, podem tornar os controles de segurança existentes ineficazes e/ou resultar no roubo dos dados do titular do cartão sem impacto perceptível no processamento normal.
Objetivo da Abordagem Personalizada	**11.5.2.b** Examine as configurações do mecanismo de detecção de mudanças para verificar se está configurado de acordo com todos os elementos especificados neste requisito.	**Práticas Recomendadas** Exemplos dos tipos de arquivos que devem ser monitorados incluem, mas não estão limitados a: • Executáveis do sistema. • Executáveis de aplicativos. • Arquivos de configuração e parâmetro. • Registros de auditoria armazenados centralmente, históricos ou arquivados. *(continua na página a seguir)*
Arquivos críticos não podem ser modificados por pessoal não autorizado sem que um alerta seja gerado.		

Requisitos e Procedimentos de Teste		Diretriz
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).		• Arquivos críticos adicionais determinados pela entidade (por exemplo, por meio de avaliação de risco ou outros meios). **Exemplos** Soluções de detecção de mudanças, como ferramentas de monitoramento de integridade de arquivo (FIM), verificam alterações, adições e exclusões em arquivos críticos e notificam quando tais alterações são detectadas.

Requisitos e Procedimentos de Teste		Diretriz
11.6 Mudanças não autorizadas nas páginas de pagamento são detectadas e respondidas.		
Requisitos da Abordagem Definida **11.6.1** Um mecanismo de detecção de mudança e violação é implantado da seguinte forma: • Para alertar o pessoal sobre modificações não autorizadas (incluindo indicadores de comprometimento, alterações, adições e exclusões) nos cabeçalhos HTTP e no conteúdo das páginas de pagamento recebidas pelo navegador do consumidor. • O mecanismo é configurado para avaliar o cabeçalho HTTP recebido e a página de pagamento. • As funções do mecanismo são realizadas da seguinte forma: – Pelo menos uma vez a cada sete dias. **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). **Objetivo da Abordagem Personalizada** O código ou as técnicas de skimming de comércio eletrônico não podem ser adicionados às páginas de pagamento recebidas pelo navegador do consumidor sem que um alerta seja gerado em tempo hábil. As medidas anti-skimming não podem ser removidas das páginas de pagamento sem que um alerta seja gerado. *(continua na página a seguir)*	**Procedimentos de Teste da Abordagem Definida** **11.6.1.a** Examine as configurações do sistema, as páginas de pagamento monitoradas e os resultados das atividades de monitoramento para verificar o uso de um mecanismo de detecção de alteração e violação. **11.6.1.b** Examine as definições de configuração para verificar se o mecanismo está configurado de acordo com todos os elementos especificados neste requisito. **11.6.1.c** Se as funções do mecanismo são realizadas em uma frequência definida pela entidade, examine a análise de risco direcionada da entidade para determinar a frequência para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1. **11.6.1.d** Examine as definições de configuração e entreviste o pessoal para verificar se as funções do mecanismo são realizadas: • Pelo menos uma vez a cada sete dias, **OU** • Na frequência definida na análise de risco direcionada da entidade realizada para este requisito.	**Objetivo** Muitas páginas web agora dependem da montagem de objetos, incluindo conteúdo ativo (principalmente JavaScript), de vários locais da Internet. Ademais, o conteúdo de muitas páginas web é definido usando gerenciamento de conteúdo e sistemas de gerenciamento de tag que podem não ser possíveis de monitorar usando mecanismos tradicionais de detecção de mudança. Portanto, o único lugar para detectar mudanças ou indicadores de atividade maliciosa é no navegador do consumidor, conforme a página é construída e todo o JavaScript interpretado. Ao comparar a versão atual do cabeçalho HTTP e o conteúdo ativo das páginas de pagamento recebidas pelo navegador do consumidor com versões anteriores ou conhecidas, é possível detectar mudanças não autorizadas que podem indicar um ataque de skimming. Ademais, procurando por indicadores conhecidos de comprometimento e elementos de script ou comportamento típico de skimmers, alertas suspeitos podem ser levantados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade A intenção deste requisito não é que uma entidade instale o software nos sistemas ou nos navegadores de seus consumidores, mas sim que a entidade use técnicas como as descritas como Exemplos na coluna Diretrizes para prevenir e detectar atividades inesperadas de script. *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.*		**Exemplos** Os mecanismos que detectam e relatam alterações nos cabeçalhos e no conteúdo da página de pagamento incluem, mas não estão limitados a: • Violações da Política de Segurança de Conteúdo (CSP) podem ser relatadas à entidade usando as diretivas *report-to ou report-uri* CSP. • Mudanças no próprio CSP podem indicar violação. • O monitoramento externo por sistemas que solicitam e analisam as páginas web recebidas (também conhecido como monitoramento de usuário sintético) pode detectar alterações no JavaScript nas páginas de pagamento e alertar o pessoal. • A incorporação de um script de detecção de violação e resistente à violação na página de pagamento pode alertar e bloquear quando o comportamento malicioso do script for detectado. • Proxies reversos e redes de entrega de conteúdo podem detectar mudanças em scripts e alertar o pessoal. Frequentemente, esses mecanismos são por assinatura ou baseados em nuvem, mas também podem ser baseados em soluções personalizadas e sob medida.

Manter uma Política de Segurança da Informação

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

Seções	
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.
12.2	Políticas de uso aceitável para tecnologias de usuário final são definidas e implementadas.
12.3	Os riscos para o ambiente de dados do titular do cartão são formalmente identificados, avaliados e gerenciados.
12.4	A conformidade com o PCI DSS é gerenciada.
12.5	O escopo do PCI DSS é documentado e validado.
12.6	A educação de conscientização sobre segurança é uma atividade contínua.
12.7	O pessoal é examinado para reduzir os riscos de ameaças internas.
12.8	O risco aos ativos de informação associados aos relacionamentos com o prestador de serviços terceirizado (TPSP) é gerenciado.
12.9	Os prestadores de serviços terceirizados (TPSPs) oferecem suporte à conformidade com o PCI DSS de seus clientes.
12.10	Incidentes de segurança suspeitos e confirmados que poderiam impactar o CDE são respondidos imediatamente.

Visão Geral

A política geral de segurança da informação da organização define o tom para toda a entidade e informa aos funcionários o que se espera deles. Todo o pessoal deve estar ciente da confidencialidade dos dados do titular do cartão e de suas responsabilidades em protegê-los.

Para os fins do Requisito 12, “pessoal” refere-se a funcionários em tempo integral e parcial, funcionários temporários, contratados e consultores com responsabilidades de segurança para proteger os dados da conta ou que podem afetar a segurança dos dados da conta.

Consulte o Apêndice G para obter as definições dos termos do PCI DSS.

Requisitos e Procedimentos de Teste		Diretriz
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.		
Requisitos da Abordagem Definida **12.1.1** Uma política geral de segurança da informação é: • Estabelecida. • Publicada. • Mantida. • Divulgada para todo o pessoal relevante, bem como para fornecedores e parceiros de negócios relevantes. **Objetivo da Abordagem Personalizada** Os objetivos e princípios estratégicos da segurança da informação são definidos, adotados e conhecidos por todo o pessoal.	**Procedimentos de Teste da Abordagem Definida** **12.1.1** Examine a documentação e entreviste o pessoal para verificar se as políticas de segurança e os procedimentos operacionais são gerenciados de acordo com todos os elementos especificados neste requisito.	**Objetivo** A política geral de segurança da informação de uma organização vincula e governa todas as outras políticas e procedimentos que definem a proteção dos dados do titular do cartão. A política de segurança da informação comunica a intenção e os objetivos da administração em relação à proteção de seus ativos mais valiosos, incluindo os dados do titular do cartão. Sem uma política de segurança da informação, os indivíduos tomarão suas próprias decisões de valor sobre os controles que são exigidos dentro da organização, o que pode fazer com que a organização não cumpra suas obrigações legais, regulamentares e contratuais, nem seja capaz de proteger adequadamente seus ativos de forma consistente. Para garantir que a política seja implementada, é importante que todo o pessoal relevante dentro da organização, bem como terceiros, fornecedores e parceiros de negócios relevantes estejam cientes da política de segurança da informação da organização e suas responsabilidades para proteger os ativos de informação. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		Práticas Recomendadas A política de segurança da organização identifica a finalidade, o escopo, a responsabilidade e as informações que definem claramente a posição da organização em relação à segurança da informação. A política geral de segurança da informação difere das políticas de segurança individuais que tratam de tecnologias ou disciplinas de segurança específicas. Esta política estabelece as diretrizes para toda a organização, enquanto as políticas de segurança individuais alinham e apoiam a política de segurança geral e comunicam objetivos específicos para as disciplinas de tecnologia ou segurança. É importante que todo o pessoal relevante dentro da organização, bem como terceiros, fornecedores e parceiros de negócios relevantes estejam cientes da política de segurança da informação da organização e suas responsabilidades para proteger os ativos de informação. **Definições** “Relevante” para este requisito significa que a política de segurança da informação é disseminada para aqueles com funções aplicáveis a alguns ou todos os tópicos da política, seja dentro da empresa ou por causa de serviços/funções desempenhados por um fornecedor ou terceiro.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **12.1.2** A política de segurança da informação é: • Revisada pelo menos uma vez a cada 12 meses. • Atualizada conforme necessário para refletir mudanças nos objetivos de negócios ou riscos ao ambiente. **Objetivo da Abordagem Personalizada** A política de segurança da informação continua refletindo os objetivos e princípios estratégicos da organização.	**Procedimentos de Teste da Abordagem Definida** **12.1.2** Examine a política de segurança da informação e entreviste o pessoal responsável para verificar se a política é gerenciada de acordo com todos os elementos especificados neste requisito.	**Objetivo** Ameaças de segurança e métodos de proteção associados evoluem rapidamente. Sem atualizar a política de segurança da informação para refletir as mudanças relevantes, novas medidas de defesa contra essas ameaças podem não ser abordadas.
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** O pessoal entende seu papel na proteção dos dados do titular do cartão da entidade	**Procedimentos de Teste da Abordagem Definida** **12.1.3.a** Examine a política de segurança da informação para verificar se ela define claramente as funções e responsabilidades da segurança da informação para todo o pessoal. **12.1.3.b** Entreviste funcionários em várias funções para verificar se eles entendem suas responsabilidades de segurança da informação. **12.1.3.c** Examine as evidências documentadas para verificar se o pessoal reconhece suas responsabilidades de segurança da informação.	**Objetivo** Sem funções de segurança claramente definidas e responsabilidades atribuídas, pode haver uso indevido dos ativos de informação da organização ou interação inconsistente com o pessoal de segurança da informação, levando à implementação insegura de tecnologias ou uso de tecnologias desatualizadas ou inseguras.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Um membro designado da gerência executiva é responsável pela segurança da informação.	**Procedimentos de Teste da Abordagem Definida** **12.1.4** Examine a política de segurança da informação para verificar se a segurança da informação foi formalmente atribuída a um diretor de segurança da informação ou outro membro da gerência executiva com conhecimento em segurança da informação.	**Objetivo** Para garantir que alguém com autoridade e responsabilidade suficientes esteja gerenciando e defendendo ativamente o programa de segurança da informação da organização, a responsabilidade pela segurança da informação deve ser atribuída no nível executivo dentro de uma organização. Os títulos comuns de gerenciamento executivo para essa função incluem Chief Information Security Officer (CISO) e Chief Security Officer (CSO - para atender a esse requisito, a função de CSO deve ser responsável pela segurança da informação). Esses cargos geralmente estão no nível mais alto da administração e fazem parte do nível executivo-chefe ou nível C, geralmente reportando-se ao CEO ou ao Conselho de Administração. **Práticas Recomendadas** As entidades também devem considerar planos de transição e/ou sucessão para esse pessoal fundamental para evitar possíveis lacunas nas atividades críticas de segurança.

Requisitos e Procedimentos de Teste		Diretriz
12.2 Políticas de uso aceitável para tecnologias de usuário final são definidas e implementadas.		
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** O uso de tecnologias de usuário final é definido e gerenciado para garantir o uso autorizado. **Observações de Aplicabilidade** Exemplos de tecnologias de usuário final para as quais políticas de uso aceitáveis são esperadas, incluindo, mas não estão limitadas a, acesso remoto e tecnologias sem fio, laptops, tablets, telefones celulares e mídia eletrônica removível, uso de e-mail e uso da Internet.	**Procedimentos de Teste da Abordagem Definida** **12.2.1** Examine as políticas de uso aceitável para tecnologias de usuário final e entrevistar o pessoal responsável para verificar se os processos estão documentados e implementados de acordo com todos os elementos especificados neste requisito.	**Objetivo** As tecnologias do usuário final são um investimento significativo e podem representar um risco significativo para uma organização se não forem gerenciadas de maneira adequada. As políticas de uso aceitável descrevem o comportamento esperado do pessoal ao usar a tecnologia da informação da organização e refletem a tolerância ao risco da organização Essas políticas instruem os funcionários sobre o que eles podem e não podem fazer com os equipamentos da empresa e instruem os funcionários sobre o uso correto e incorreto dos recursos de Internet e e-mail da empresa. Essas políticas podem proteger legalmente uma organização e permitir que ela atue quando as políticas forem violadas. **Práticas Recomendadas** É importante que as políticas de uso sejam apoiadas por controles técnicos para gerenciar a aplicação das políticas. Estruturar políticas como requisitos simples do tipo “fazer” e “não fazer” vinculados a uma finalidade pode ajudar a remover a ambiguidade e fornecer ao pessoal o contexto para o requisito.

Requisitos e Procedimentos de Teste		Diretriz
12.3 Os riscos para o ambiente de dados do titular do cartão são formalmente identificados, avaliados e gerenciados.		
Requisitos da Abordagem Definida **12.3.1** Cada requisito PCI DSS que fornece flexibilidade para a frequência com que é realizado (por exemplo, requisitos a serem realizados periodicamente) é apoiado por uma análise de risco direcionada que é documentada e inclui: • Identificação dos ativos 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 a frequência com que o requisito deve ser executado para minimizar a probabilidade 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. **Objetivo da Abordagem Personalizada** Conhecimento atualizado e avaliação de riscos para o CDE são mantidos.	**Procedimentos de Teste da Abordagem Definida** **12.3.1** Examine as políticas e procedimentos documentados para verificar se um processo está definido para realizar análises de risco direcionadas para cada requisito do PCI DSS que fornece flexibilidade para a frequência com que o requisito é executado e se o processo inclui todos os elementos especificados neste requisito.	**Objetivo** Alguns requisitos do PCI DSS permitem que uma entidade defina a frequência com que uma atividade é realizada com base no risco para o ambiente. A realização desta análise de risco de acordo com uma metodologia garante a validade e consistência com as políticas e procedimentos. Essa análise de risco direcionada (em oposição a uma avaliação de risco tradicional em toda a empresa) concentra-se nos requisitos do PCI DSS que permitem a flexibilidade de uma entidade sobre a frequência com que uma entidade executa um determinado controle. Para essa análise de risco, a entidade avalia cuidadosamente cada requisito do PCI DSS que fornece essa flexibilidade e determina a frequência que oferece suporte à segurança adequada para a entidade e o nível de risco que a entidade está disposta a aceitar. A análise de risco identifica os ativos específicos, como os componentes de sistema e dados - por exemplo, arquivos de registro ou credenciais - que o requisito se destina a proteger, bem como a(s) ameaça(s) ou resultados contra quem o requisito está protegendo os ativos, por exemplo, malware, um intruso não detectado ou uso indevido de credenciais Exemplos de fatores que podem contribuir para a probabilidade ou impacto incluem qualquer um que possa aumentar a vulnerabilidade de um ativo a uma ameaça - por exemplo, exposição a redes não confiáveis, complexidade do ambiente ou alta rotatividade de pessoal - bem como a criticidade dos componentes de sistema, ou volume e sensibilidade dos dados sendo protegidos. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
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.*		A revisão dos resultados dessas análises de risco direcionadas pelo menos uma vez a cada 12 meses e sobre as mudanças que poderiam impactar o risco ao ambiente permite que a organização garanta que os resultados da análise de risco permaneçam atualizados com as mudanças organizacionais e as ameaças, tendências e tecnologias em evolução, e que as frequências selecionadas ainda abordam adequadamente o risco da entidade. **Práticas Recomendadas** Uma avaliação de risco em toda a empresa, que é uma atividade pontual que permite às entidades identificar ameaças e vulnerabilidades associadas, é recomendada, mas não é necessária para que as entidades determinem e entendam ameaças emergentes mais amplas com potencial de impactar negativamente seu negócio. Essa avaliação de risco em toda a empresa pode ser estabelecida como parte de um programa de gerenciamento de risco abrangente que é usado como uma entrada para a revisão anual da política geral de segurança da informação de uma organização (consulte o Requisito 12.1.1). Exemplos de metodologias de avaliação de risco para avaliações de risco em toda a empresa incluem, mas não estão limitados a, ISO *27005 e* NIST *SP 800-30.*

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.3.2 Uma análise de risco direcionada é realizada para cada requisito do PCI DSS que a entidade atende com a abordagem personalizada, para incluir: • Evidência documentada detalhando cada elemento especificado no Apêndice D: Abordagem personalizada (incluindo, no mínimo, uma matriz de controles e análise de risco). • Aprovação de evidências documentadas pela alta administração. • Execução da análise de risco direcionada pelo menos uma vez a cada 12 meses.	**12.3.2** Examine a análise de risco direcionada documentada para cada requisito do PCI DSS que a entidade atende com a abordagem personalizada para verificar se a documentação para cada requisito existe e está de acordo com todos os elementos especificados neste requisito.	Uma análise de risco seguindo uma metodologia robusta e repetível permite que uma entidade atenda ao objetivo da abordagem personalizada. **Definições** A abordagem personalizada para atender a um requisito PCI DSS permite que as entidades definam os controles usados para atender ao objetivo da abordagem personalizada declarado de um determinado requisito de uma forma que não siga estritamente o requisito definido. Espera-se que esses controles atendam ou excedam, pelo menos, a segurança fornecida pelo requisito definido e exijam ampla documentação por parte da entidade usando a abordagem personalizada. **Informações Adicionais** Consulte o Apêndice D: Abordagem Personalizada para obter instruções sobre como documentar as evidências necessárias para a abordagem personalizada. Consulte o Apêndice E: Modelos de Amostra para Apoiar a Abordagem Personalizada para modelos que as entidades podem usar para documentar seus controles personalizados. Observe que, embora o uso dos modelos seja opcional, as informações especificadas em cada modelo devem ser documentadas e fornecidas ao assessor de cada entidade.
Objetivo da Abordagem Personalizada		
Esse requisito faz parte da abordagem personalizada e deve ser atendido para aqueles que usam a abordagem personalizada.		
Observações de Aplicabilidade		
Este requisito se aplica apenas a entidades que usam uma abordagem personalizada.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **12.3.3** Conjuntos de criptografia *(cipher suites)* 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 criptografia e protocolos em uso, incluindo a finalidade e onde são usados. • Monitoramento ativo das tendências da indústria em relação à viabilidade contínua de todos conjuntos de criptografia e protocolos em uso. • Uma estratégia documentada para responder às mudanças previstas nas vulnerabilidades criptográficas. **Objetivo da Abordagem Personalizada** A entidade é capaz de responder rapidamente a quaisquer vulnerabilidades em protocolos ou algoritmos criptográficos, onde essas vulnerabilidades afetam a proteção dos dados do titular do cartão. **Observações de Aplicabilidade** O requisito se aplica a todos os conjuntos de criptografia e protocolos usados para atender aos requisitos 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.*	**Procedimentos de Teste da Abordagem Definida** **12.3.3** Examine a documentação dos conjuntos de criptografia e protocolos em uso e entreviste o pessoal para verificar se a documentação e a revisão estão de acordo com todos os elementos especificados neste requisito.	**Objetivo** Os protocolos e os pontos fortes da criptografia podem mudar rapidamente ou ser descontinuados devido à identificação de vulnerabilidades ou falhas de projeto. Para oferecer suporte às necessidades de segurança de dados atuais e futuras, as entidades precisam saber onde a criptografia é usada e compreender como seriam capazes de responder rapidamente às mudanças que afetam a força de suas implementações criptográficas. **Práticas Recomendadas** A agilidade criptográfica é importante para garantir que uma alternativa ao método de criptografia original ou primitiva criptográfica esteja disponível, com planos de atualização para a alternativa sem alterações significativas na infraestrutura do sistema. Por exemplo, se a entidade estiver ciente de quando os protocolos ou algoritmos serão reprovados por órgãos de padrões, ela pode fazer planos proativos para atualizar antes que a reprovação tenha impacto nas operações. **Definições** “Agilidade criptográfica” refere-se à capacidade de monitorar e gerenciar a criptografia e as tecnologias de verificação relacionadas implantadas em uma organização. **Informações Adicionais** Consulte *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 da indústria 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".	**12.3.4** Examine a documentação para a revisão das tecnologias de hardware e software em uso e entreviste o pessoal para verificar se a revisão está de acordo com todos os elementos especificados neste requisito.	As tecnologias de hardware e software estão em constante evolução, e as organizações precisam estar cientes das mudanças nas tecnologias que usam, bem como das ameaças em evolução a essas tecnologias para garantir que possam se preparar e gerenciar vulnerabilidades em hardware e software que não serão corrigidas pelo fornecedor ou desenvolvedor. **Práticas Recomendadas** As organizações devem revisar as versões do firmware para garantir que permaneçam atuais e com suporte dos fornecedores. As organizações também precisam estar cientes das mudanças feitas pelos fornecedores de tecnologia em seus produtos ou processos para entender como tais mudanças podem impactar o uso da tecnologia pela organização. As análises regulares das tecnologias que impactam ou influenciam os controles do PCI DSS podem ajudar nas estratégias de compra, uso e implantação, e garantir que os controles que dependem dessas tecnologias permaneçam eficazes. Essas revisões incluem, mas não se limitam a, revisar tecnologias que não são mais suportadas pelo fornecedor e/ou não atendem mais às necessidades de segurança da organização.
Objetivo da Abordagem Personalizada		
As tecnologias de hardware e software da entidade são atualizadas e suportadas pelo fornecedor. Os planos para remover ou substituir todos os componentes do sistema sem suporte são revisados periodicamente.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
12.4 A conformidade com o PCI DSS é gerenciada.		
Requisitos da Abordagem Definida **12.4.1** ***Requisito adicional apenas para prestadores de serviços:*** A responsabilidade é estabelecida pela gestão executiva para a proteção dos dados do titular do cartão e um programa de conformidade com o PCI DSS para incluir: • Responsabilidade geral para manter a conformidade com o PCI DSS. • Definição de um estatuto para um programa de conformidade com o PCI DSS e comunicação para a gestão executiva. **Objetivo da Abordagem Personalizada** Os executivos são responsáveis pela segurança dos dados do titular do cartão. **Observações de Aplicabilidade** Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. A gestão executiva pode incluir cargos de nível C, conselho de administração ou equivalente. Os títulos específicos dependerão da estrutura organizacional específica. A responsabilidade pelo programa de conformidade com o PCI DSS pode ser atribuída a funções individuais e/ou a unidades de negócios dentro da organização.	**Procedimentos de Teste da Abordagem Definida** **12.4.1** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine a documentação para verificar se a gestão executiva estabeleceu a responsabilidade pela proteção dos dados do titular do cartão e um programa de conformidade com o PCI DSS de acordo com todos os elementos especificados neste requisito.	**Objetivo** A atribuição de responsabilidades de conformidade com o PCI DSS pela gestão executiva garante a visibilidade de nível executivo do programa de conformidade com o PCI DSS e permite a oportunidade de fazer perguntas apropriadas para determinar a eficácia do programa e influenciar as prioridades estratégicas.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.4.2 ***Requisito adicional apenas para prestadores de serviços:*** As análises são realizadas pelo menos uma vez a cada três meses para confirmar que a equipe está desempenhando suas tarefas de acordo com todas as políticas de segurança e procedimentos operacionais. –As análises são realizadas por pessoal que não seja o responsável pela execução da tarefa e incluindo, mas não se limitando às seguintes tarefas: • Revisões diárias do registro. • Revisões de configuração para controles de segurança de rede. • Aplicando padrões de configuração a novos sistemas. • Respondendo a alertas de segurança. • Processos de gerenciamento de mudanças.	**12.4.2.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as políticas e procedimentos para verificar se os processos estão definidos para a realização de análises para confirmar se o pessoal está executando suas tarefas de acordo com todas as políticas de segurança e todos os procedimentos operacionais, incluindo, mas não se limitando às tarefas especificadas neste requisito.	A confirmação regular de que as políticas e procedimentos de segurança estão sendo seguidos fornece a garantia de que os controles esperados estão ativos e funcionando conforme pretendido Este requisito é diferente de outros requisitos que especificam uma tarefa a ser executada. O objetivo dessas revisões não é realizar novamente outros requisitos do PCI DSS, mas confirmar se as atividades de segurança estão sendo executadas continuamente. **Práticas Recomendadas** Essas revisões também podem ser usadas para verificar se a evidência apropriada está sendo mantida - por exemplo, registros de auditoria, relatórios de varredura de vulnerabilidade, revisões de conjuntos de regras de controle de segurança de rede - para auxiliar na preparação da entidade para sua próxima avaliação do PCI DSS. **Exemplos** Tomando o Requisito 1.2.7 como um exemplo, o Requisito 12.4.2 é atendido pela confirmação, pelo menos uma vez a cada três meses, de que as revisões das configurações dos controles de segurança da rede ocorreram na frequência necessária. Por outro lado, o Requisito 1.2.7 é atendido pela revisão das configurações conforme especificado no requisito.
Objetivo da Abordagem Personalizada A eficácia operacional dos controles críticos do PCI DSS é verificada periodicamente por inspeção manual dos registros.	**12.4.2.b** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Entreviste o pessoal responsável e examine os registros das revisões para verificar se as revisões são realizadas: • Pelo menos uma vez a cada três meses. • Por pessoal que não seja o responsável pela execução de determinada tarefa.	
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.4.2.1 ***Requisito adicional apenas para prestadores de serviços:*** As análises realizadas de acordo com o Requisito 12.4.2 são documentadas para incluir: • Resultados das revisões. • Ações de correção documentadas tomadas para quaisquer tarefas que não foram realizadas no Requisito 12.4.2. • Revisão e aprovação dos resultados pela equipe com responsabilidade pelo programa de conformidade com o PCI DSS.	**12.4.2.1** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine a documentação das análises conduzidas de acordo com o Requisito 12.4.2 do PCI DSS para verificar se a documentação inclui todos os elementos especificados neste requisito.	A intenção dessas verificações independentes é confirmar se as atividades de segurança estão sendo realizadas de forma contínua. Essas revisões também podem ser usadas para verificar se a evidência apropriada está sendo mantida - por exemplo, registros de auditoria, relatórios de varredura de vulnerabilidade, revisões de conjuntos de regras de controle de segurança de rede - para auxiliar na preparação da entidade para sua próxima avaliação do PCI DSS.
Objetivo da Abordagem Personalizada		
As conclusões das análises de eficácia operacional são avaliadas pela administração; atividades de remediação apropriadas são implementadas.		
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

Requisitos e Procedimentos de Teste		Diretriz
12.5 O escopo do PCI DSS é documentado e validado.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Manter uma lista atual de todos os componentes de sistema permitirá que uma organização defina o escopo de seu ambiente e implemente os requisitos do PCI DSS com precisão e eficiência. Sem um inventário, alguns componentes de sistema podem ser negligenciados e excluídos inadvertidamente dos padrões de configuração da organização. **Práticas Recomendadas** Se uma entidade mantém um inventário de todos os ativos, os componentes de sistema no escopo do PCI DSS devem ser claramente identificáveis entre os outros ativos. Os inventários devem incluir containers ou imagens que podem ser instanciadas. Atribuir um proprietário ao inventário ajuda a garantir que o inventário permaneça atualizado. **Exemplos** Os métodos para manter um inventário incluem um banco de dados, uma série de arquivos ou uma ferramenta de gerenciamento de inventário.
12.5.1 Um inventário dos componentes de sistema que estão no escopo do PCI DSS, incluindo uma descrição de função/uso, é mantido e atualizado.	**12.5.1.a** Examine o inventário para verificar se ele inclui todos os componentes de sistema dentro do escopo e uma descrição da função/uso de cada um.	
	12.5.1.b Entreviste a equipe para verificar se o inventário é mantido atualizado.	
Objetivo da Abordagem Personalizada		
Todos os componentes de sistema no escopo do PCI DSS são identificados e conhecidos.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
12.5.2 O escopo do PCI DSS é documentado e confirmado pela entidade pelo menos uma vez a cada 12 meses e em consequência de mudança significativa no ambiente dentro do escopo. 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 não-presente e comércio eletrônico). • Atualizar todos os diagramas de fluxo de dados de acordo com o 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 de 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. • Confirmar se todos os fluxos de dados identificados, dados da conta, componentes de sistema, controles de segmentação e conexões de terceiros com acesso ao CDE estão incluídos no escopo.	**12.5.2.a** Examine os resultados documentados das revisões do escopo e entreviste o pessoal para verificar se as revisões são realizadas: • Pelo menos uma vez a cada 12 meses. • Após mudanças significativas no ambiente dentro do escopo. **12.5.2.b** Examine os resultados documentados das revisões de escopo realizadas pela entidade para verificar se a atividade de confirmação de escopo do PCI DSS inclui todos os elementos especificados neste requisito.	**Objetivo** A validação frequente do escopo do PCI DSS ajuda a garantir que o escopo do PCI DSS permaneça atualizado e alinhado com os objetivos de negócios em constante mudança e, portanto, que os controles de segurança estejam protegendo todos os componentes apropriados de sistema. **Práticas Recomendadas** O escopo preciso envolve a avaliação crítica do CDE e de todos os componentes de sistema conectados para determinar a cobertura necessária para os requisitos do PCI DSS. As atividades de definição do escopo, incluindo uma análise cuidadosa e monitoramento contínuo, ajudam a garantir que os sistemas dentro do escopo sejam devidamente protegidos. Ao documentar a localização dos dados da conta, a entidade pode considerar a criação de uma tabela ou planilha que inclua as seguintes informações: • Armazenamentos de dados (bancos de dados, arquivos, nuvem, etc.), incluindo a finalidade de armazenamento de dados e o período de retenção, • Quais elementos do CHD são armazenados (PAN, data de validade, nome do titular do cartão e/ou quaisquer elementos do SAD antes da conclusão da autorização), • Como os dados são protegidos (tipo de criptografia e força, algoritmo de hash e força, truncamento, tokenização), • Como o acesso aos armazenamentos de dados é registrado, incluindo uma descrição do(s) mecanismo(s) de registro em uso (solução corporativa, nível de aplicativo, nível de sistema operacional etc.). *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada O escopo do PCI DSS é verificado periodicamente, e após mudanças significativas, por uma análise abrangente e medidas técnicas apropriadas. **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.		Além de sistemas e redes internos, todas as conexões de entidades terceirizadas - por exemplo, parceiros de negócios, entidades que fornecem serviços de suporte remoto e outros prestadores de serviços - precisam ser identificadas para determinar a inclusão no escopo do PCI DSS. Uma vez que as conexões dentro do escopo tenham sido identificadas, os controles do PCI DSS aplicáveis podem ser implementados para reduzir o risco de uma conexão de terceiros ser usada para comprometer o CDE de uma entidade. Uma ferramenta ou metodologia de descoberta de dados pode ser usada para facilitar a identificação de todas as fontes e locais de PAN e para procurar PAN que reside em sistemas e redes fora do CDE atualmente definido ou em locais inesperados dentro do CDE definido - por exemplo, em um registro de erro ou arquivo de despejo de memória. Essa abordagem pode ajudar a garantir que locais anteriormente desconhecidos do PAN sejam detectados e que o PAN seja eliminado ou devidamente protegido. **Informações Adicionais** Para obter orientações adicionais, consulte o *Suplemento de Informações: Orientação para Escopo e Segmentação de Rede do PCI DSS.*

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.5.2.1 ***Requisito adicional apenas para prestadores de serviços:*** O escopo do PCI DSS é documentado e confirmado pela entidade pelo menos uma vez a cada seis meses e em consequência de mudança significativa no ambiente dentro do escopo. No mínimo, a validação do escopo inclui todos os elementos especificados no Requisito 12.5.2.	**12.5.2.1.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine os resultados documentados das revisões de escopo e entreviste o pessoal para verificar se as revisões de acordo com o Requisito 12.5.2 são realizadas: • Pelo menos uma vez a cada seis meses, e • Após mudança significativa	Os prestadores de serviços normalmente têm acesso a maiores volumes de dados do titular do cartão do que os comerciantes, ou podem fornecer um ponto de entrada que pode ser explorado para comprometer várias outras entidades. Os prestadores de serviços também costumam ter redes maiores e mais complexas, sujeitas a alterações mais frequentes. A probabilidade de mudanças negligenciadas no escopo em redes complexas e dinâmicas é maior nos ambientes dos prestadores de serviços. Validar o escopo do PCI DSS com mais frequência provavelmente descobrirá essas alterações negligenciadas antes que possam ser exploradas por um atacante.
Objetivo da Abordagem Personalizada	**12.5.2.1.b** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine os resultados documentados das revisões do escopo para verificar se a validação do escopo inclui todos os elementos especificados no Requisito 12.5.2.	
A precisão do escopo do PCI DSS é verificada para ser continuamente precisa por uma análise abrangente e medidas técnicas apropriadas.		
Observações de Aplicabilidade		
Este requisito se aplica somente quando a entidade que está sendo avaliada é uma prestadora de serviços. *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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A estrutura e a gestão de uma organização definem os requisitos e protocolo para operações eficazes e seguras. Mudanças nessa estrutura podem ter efeitos negativos nos controles e estruturas existentes, realocando ou removendo recursos que antes suportavam os controles do PCI DSS ou herdando novas responsabilidades que podem não ter estabelecido controles implementados. Portanto, é importante revisitar o escopo e os controles do PCI DSS quando houver mudanças na estrutura e no gerenciamento de uma organização para garantir que os controles estejam implementados e ativos. **Exemplos** Mudanças na estrutura organizacional incluem, mas não estão limitadas a, fusões ou aquisições de empresas e mudanças significativas ou realocações de pessoal com responsabilidade pelos controles de segurança.
12.5.3 ***Requisito adicional apenas para prestadores de serviços:*** Mudanças significativas na estrutura organizacional resultam em uma revisão documentada (interna) do impacto no escopo do PCI DSS e na aplicabilidade dos controles, com os resultados comunicados à gestão executiva.	**12.5.3.a** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as políticas e procedimentos para verificar se os processos estão definidos de forma que uma mudança significativa na estrutura organizacional resulte em uma revisão documentada do impacto no escopo do PCI DSS e na aplicabilidade dos controles.	
Objetivo da Abordagem Personalizada O escopo do PCI DSS é confirmado após uma mudança organizacional significativa.	**12.5.3.b** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine a documentação (por exemplo, atas de reunião) e entreviste o pessoal responsável para verificar se as mudanças significativas na estrutura organizacional resultaram em revisões documentadas que incluíram todos os elementos especificados neste requisito, com os resultados comunicados à gestão executiva.	
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. *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.*		

Requisitos e Procedimentos de Teste		Diretriz
12.6 A educação de conscientização sobre segurança é uma atividade contínua.		
Requisitos da Abordagem Definida **12.6.1** Um programa formal de conscientização sobre 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. **Objetivo da Abordagem Personalizada** O pessoal está bem informado sobre o cenário de ameaças, sua responsabilidade pela operação dos controles de segurança relevantes e é capaz de acessar assistência e orientação quando necessário.	**Procedimentos de Teste da Abordagem Definida** **12.6.1** Examine o programa de conscientização sobre segurança para verificar se ele fornece conscientização a todos os funcionários sobre a política e procedimentos de segurança da informação da entidade e o papel do pessoal na proteção dos dados do titular do cartão.	**Objetivo** Se o pessoal não for informado sobre as políticas e procedimentos de segurança da informação de sua empresa e suas próprias responsabilidades de segurança, as proteções e processos de segurança que foram implementados podem se tornar ineficazes por meio de erros não intencionais ou ações intencionais.
Requisitos da Abordagem Definida **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 do CDE da entidade ou as informações fornecidas ao pessoal sobre sua função na proteção dos dados do titular do cartão.	**Procedimentos de Teste da Abordagem Definida** **12.6.2** Examine o conteúdo do programa de conscientização sobre segurança, evidências de revisões e entreviste o pessoal para verificar se o programa de conscientização sobre segurança está de acordo com todos os elementos especificados neste requisito.	**Objetivo** O ambiente de ameaça e as defesas de uma entidade não são estáticos. Como tal, os materiais do programa de conscientização sobre segurança devem ser atualizados com a frequência necessária para garantir que a educação recebida pelo pessoal esteja atualizada e represente o ambiente de ameaça atual.

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada O conteúdo do material de conscientização sobre segurança é revisado e atualizado periodicamente. **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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O treinamento do pessoal garante que eles recebam informações sobre a importância da segurança da informação e que entendam seu papel na proteção da organização. Exigir o reconhecimento do pessoal ajuda a garantir que eles leram e compreenderam as políticas e procedimentos de segurança e que assumiram e continuarão a se comprometer em cumprir essas políticas. **Práticas Recomendadas** As entidades podem incorporar o treinamento de novos contratados como parte do processo de integração de Recursos Humanos. O treinamento deve delinear os itens “fazer” e “não fazer” relacionados à segurança. O treinamento de atualização periódica reforça os principais processos e procedimentos de segurança que podem ser esquecidos ou ignorados. As entidades devem considerar a exigência de treinamento de conscientização sobre segurança sempre que o pessoal for transferido para funções em que possam afetar a segurança dos dados da conta de funções nas quais eles não tiveram esse impacto. Os métodos e o conteúdo do treinamento podem variar, dependendo das funções do pessoal. **Exemplos** Os diferentes métodos que podem ser usados para fornecer conscientização e educação sobre segurança incluem pôsteres, cartas, treinamento online, treinamento presencial, reuniões de equipe e incentivos. Reconhecimentos de pessoal podem ser registrados por escrito ou eletronicamente.
12.6.3 O pessoal recebe treinamento de conscientização sobre 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.	**12.6.3.a** Examine os registros do programa de conscientização sobre segurança para verificar se o pessoal participa do treinamento de conscientização sobre segurança na contratação e pelo menos uma vez a cada 12 meses.	
	12.6.3.b Examine os materiais do programa de conscientização sobre segurança para verificar se o programa inclui vários métodos de comunicação de conscientização e treinamento de pessoal.	
	12.6.3.c Entreviste a equipe para verificar se ela concluiu o treinamento de conscientização e está ciente de sua função na proteção dos dados do titular do cartão.	
	12.6.3.d Examine os materiais do programa de conscientização sobre segurança e reconhecimentos de pessoal para verificar se os funcionários reconhecem, pelo menos uma vez a cada 12 meses, que leram e compreenderam a política e os procedimentos de segurança da informação.	
Objetivo da Abordagem Personalizada		
O pessoal permanece informado sobre o cenário de ameaças, sua responsabilidade pela operação dos controles de segurança relevantes e é capaz de acessar assistência e orientação quando necessário.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **12.6.3.1** O treinamento de conscientização sobre segurança inclui a conscientização de ameaças e vulnerabilidades que podem impactar a segurança do CDE, incluindo, mas não se limitando a: • Phishing e ataques relacionados. • Engenharia social. **Objetivo da Abordagem Personalizada** O pessoal está bem informado sobre suas próprias vulnerabilidades humanas e como os atores da ameaça tentarão explorar tais vulnerabilidades. O pessoal pode ter acesso à assistência e orientação quando necessário. **Observações de Aplicabilidade** Consulte o Requisito 5.4.1 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 sobre segurança incluindo 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.*	**Procedimentos de Teste da Abordagem Definida** **12.6.3.1** Examine o conteúdo do treinamento de conscientização sobre segurança para verificar se ele inclui todos os elementos especificados neste requisito.	**Objetivo** Educar a equipe sobre como detectar, reagir e relatar possíveis ataques de phishing e ataques relacionados e tentativas de engenharia social é essencial para minimizar a probabilidade de ataques bem-sucedidos. **Práticas Recomendadas** Um programa de conscientização de segurança eficaz deve incluir exemplos de e-mails de phishing e testes periódicos para determinar a prevalência de funcionários que relatam tais ataques. O material de treinamento que uma entidade pode considerar para este tópico inclui: • Como identificar phishing e outros ataques de engenharia social. • Como reagir a suspeitas de phishing e engenharia social. • Onde e como denunciar suspeita de atividade de phishing e engenharia social. Uma ênfase em reportar permite que a organização recompense o comportamento positivo, otimize as defesas técnicas (consulte o Requisito 5.4.1) e tome medidas imediatas para remover e-mails de phishing semelhantes que escaparam das defesas técnicas das caixas de entrada dos destinatários.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.6.3.2 O treinamento de conscientização sobre segurança inclui a conscientização sobre o uso aceitável de tecnologias de usuário final de acordo com o Requisito 12.2.1.	**12.6.3.2** Examine o conteúdo do treinamento de conscientização sobre segurança para verificar se inclui a conscientização sobre o uso aceitável de tecnologias de usuário final de acordo com o Requisito 12.2.1.	Ao incluir os pontos fundamentais da política de uso aceitável no treinamento regular e no contexto relacionado, o pessoal compreenderá suas responsabilidades e como elas impactam a segurança dos sistemas de uma organização.
Objetivo da Abordagem Personalizada		
Os funcionários estão bem informados sobre sua responsabilidade pela segurança e operação das tecnologias do usuário final e podem acessar assistência e orientação quando necessário.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
12.7 O pessoal é examinado para reduzir os riscos de ameaças internas.		
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** O risco relacionado ao acesso de novos membros da equipe ao CDE é compreendido e gerenciado. **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.	**Procedimentos de Teste da Abordagem Definida** **12.7.1** Entreviste a gerência do departamento de Recursos Humanos responsável para verificar se a triagem é conduzida, dentro das restrições das leis locais, antes de contratar pessoal potencial que terá acesso ao CDE.	**Objetivo** A realização de uma triagem completa antes de contratar pessoal potencial que deverá ter acesso ao CDE fornece às entidades as informações necessárias para tomar decisões de risco informadas em relação ao pessoal que contratam que terá acesso ao CDE. Outros benefícios da triagem de pessoal potencial incluem ajudar a garantir a segurança no local de trabalho e confirmar as informações fornecidas por funcionários em potencial em seus currículos. **Práticas Recomendadas** As entidades devem considerar a triagem de pessoal existente sempre que forem transferidos para funções nas quais tenham acesso ao CDE de funções nas quais não tenham esse acesso. Para ser eficaz, o nível de triagem deve ser apropriado para a posição. Por exemplo, os cargos que exigem maior responsabilidade ou que têm acesso administrativo a dados ou sistemas críticos podem justificar uma triagem mais detalhada ou mais frequente do que os cargos com menos responsabilidade e acesso. **Exemplos** As opções de triagem podem incluir, conforme apropriado para a região da entidade, histórico de empregos anteriores, revisão de informações públicas/recursos de mídia social, antecedentes criminais, histórico de crédito e verificações de referência.

Requisitos e Procedimentos de Teste		Diretriz
12.8 O risco aos ativos de informação associados aos relacionamentos com o prestador de serviços terceirizado (TPSP) é gerenciado.		
Requisitos da Abordagem Definida **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 fornecidos. **Objetivo da Abordagem Personalizada** São mantidos registros dos TPSPs e dos serviços prestados. **Observações de Aplicabilidade** O uso de um TPSP em conformidade com o PCI DSS não torna uma entidade em conformidade com o PCI DSS, nem remove a responsabilidade da entidade por sua própria conformidade com o PCI DSS.	**Procedimentos de Teste da Abordagem Definida** **12.8.1.a** Examine as políticas e procedimentos para verificar se os processos são definidos para manter uma lista de TPSPs, incluindo uma descrição para cada um dos serviços prestados, para todos os TPSPs com os quais os dados da conta são compartilhados ou que podem afetar a segurança dos dados da conta. **12.8.1.b** Examine a documentação para verificar se uma lista de todos os TPSPs é mantida e inclui uma descrição dos serviços prestados.	**Objetivo** Manter uma lista de todos os TPSPs identifica onde o risco potencial se estende para fora da organização e define a superfície de ataque estendida da organização. **Exemplos** Diferentes tipos de TPSPs incluem aqueles que: • Armazena, processa ou transmite dados da conta em nome da entidade (como gateways de pagamento, processadores de pagamento, prestadores de serviços de pagamento (PSPs) e provedores de armazenamento externo). • Gerenciam os componentes do sistema incluídos na avaliação do PCI DSS da entidade (como prestadores de serviços de controle de segurança de rede, serviços antimalware e sistemas de gerenciamento de eventos e informações de segurança (SIEM); centros de contato e call centers; empresas de hospedagem na web; e provedores de nuvem IaaS, PaaS, SaaS e FaaS). • Podem impactar a segurança do CDE da entidade (como fornecedores que fornecem suporte por meio de acesso remoto e desenvolvedores de software sob medida).

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.8.2 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. • Os 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 possam impactar a segurança do CDE da entidade.	**12.8.2.a** Examine as políticas e procedimentos para verificar se os processos são definidos para manter acordos escritos com todos os TPSPs de acordo com todos os elementos especificados neste requisito.	O reconhecimento por escrito de um TPSP demonstra seu compromisso em manter a segurança adequada dos dados da conta que obtém de seus clientes e que o TPSP está totalmente ciente dos ativos que podem ser afetados durante a prestação do serviço do TPSP. Até que ponto um TPSP específico é responsável pela segurança dos dados da conta dependerá do serviço prestado e do acordo entre o provedor e a entidade avaliada (o cliente). Em conjunto com o Requisito 12.9.1, este requisito visa promover um nível consistente de entendimento entre as partes sobre suas responsabilidades aplicáveis do PCI DSS. Por exemplo, o contrato pode incluir os requisitos aplicáveis do PCI DSS a serem mantidos como parte do serviço prestado.
Objetivo da Abordagem Personalizada	**12.8.2.b** Examine os acordos escritos com os TPSPs para verificar se eles são mantidos de acordo com todos os elementos especificados neste requisito.	**Práticas Recomendadas** A entidade também pode querer considerar a inclusão em seu contrato por escrito com um TPSP de que o TPSP apoiará a solicitação de informações da entidade de acordo com o Requisito 12.9.2. As entidades também vão querer entender se algum TPSP tem relacionamentos “aninhados” com outros TPSPs, ou seja, os contratos de TPSP primários com outro(s) TPSP(s) para fins de fornecimento de um serviço. É importante entender se o TPSP primário está contando com o(s) TPSP(s) secundário(s) para atingir a conformidade geral de um serviço e que tipos de acordos escritos o TPSP primário tem em vigor com os TPSPs secundários. As entidades podem considerar a inclusão de cobertura em seu contrato por escrito para quaisquer TPSPs “aninhados” que um TPSP principal possa usar. *(continua na página a seguir)*
São mantidos registros do reconhecimento de cada TPSP de sua responsabilidade de proteger os dados da conta.		

Requisitos e Procedimentos de Teste		Diretriz
Observações de Aplicabilidade A redação exata de um reconhecimento dependerá do acordo entre as duas partes, dos detalhes do serviço prestado e das responsabilidades atribuídas a cada uma das partes. O reconhecimento não precisa incluir a redação exata fornecida neste requisito. A evidência de que um TPSP está atendendo aos requisitos do PCI DSS (por exemplo, um Atestado de Conformidade do PCI DSS (AOC) ou uma declaração no site de uma empresa) não é o mesmo que um acordo escrito especificado neste requisito.		**Informações Adicionais** Consulte o *"Suplemento de Informações: Garantia de Segurança de Terceiros* para obter mais orientações.
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Um processo completo para envolver os TPSPs, incluindo detalhes para seleção e verificação antes do envolvimento, ajuda a garantir que um TPSP seja completamente examinado internamente por uma entidade antes de estabelecer um relacionamento formal e que o risco para os dados do titular do cartão associados ao envolvimento do TPSP é entendido. **Práticas Recomendadas** Os processos e metas de due diligence específicos variam para cada organização. Os elementos que devem ser considerados incluem as práticas de relatório do provedor, procedimentos de notificação de violação e resposta a incidentes, detalhes de como as responsabilidades do PCI DSS são atribuídas entre cada parte, como o TPSP valida sua conformidade com o PCI DSS e quais evidências eles fornecem.
12.8.3 Um processo estabelecido é implementado para envolver os TPSPs, incluindo a due diligence antes do envolvimento.	**12.8.3.a** Examine as políticas e procedimentos para verificar se os processos estão definidos para envolver os TPSPs, incluindo a due diligence antes do envolvimento.	
	12.8.3.b Analisar as evidências e entrevistar o pessoal responsável para verificar se o processo de contratação de TPSPs inclui a due diligence antes da contratação.	
Objetivo da Abordagem Personalizada A capacidade, intenção e recursos de um potencial TPSP para proteger adequadamente os dados da conta são avaliados antes que o TPSP seja contratado.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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.	**12.8.4.a** Examine as políticas e procedimentos para verificar se os processos são definidos para monitorar o status de conformidade do PCI DSS dos TPSPs pelo menos uma vez a cada 12 meses.	Saber o status de conformidade do PCI DSS de todos os TPSPs envolvidos fornece garantia e consciência sobre se eles estão em conformidade com os requisitos aplicáveis aos serviços que oferecem à organização. **Práticas Recomendadas** Se o TPSP oferece uma variedade de serviços, o status de conformidade que a entidade monitora deve ser específico para os serviços prestados à entidade e os serviços no escopo da avaliação do PCI DSS da entidade. Se um TPSP tiver um Atestado de Conformidade do PCI DSS (AOC), a expectativa é que o TPSP forneça isso aos clientes, mediante solicitação, para demonstrar seu status de conformidade com o PCI DSS. Se o TPSP não passou por uma avaliação do PCI DSS, ele pode fornecer outras evidências suficientes para demonstrar que atendeu aos requisitos aplicáveis sem passar por uma validação de conformidade formal. Por exemplo, o TPSP pode fornecer evidências específicas ao assessor da entidade para que o assessor possa confirmar que os requisitos aplicáveis foram atendidos. Alternativamente, o TPSP pode optar por se submeter a várias avaliações sob demanda por cada um dos assessores de seus clientes, com cada avaliação direcionada para confirmar se os requisitos aplicáveis sejam atendidos. **Informações Adicionais** Para obter mais informações sobre prestadores de serviços terceirizados, consulte: • Seção PCI DSS: *Uso de Prestadores de Serviço Terceirizados.* • *Suplemento de Informações: Garantia de Segurança de Terceiros*.
Objetivo da Abordagem Personalizada	**12.8.4.b** Examine a documentação e entreviste a equipe responsável para verificar se o status de conformidade do PCI DSS de cada TPSP é monitorado pelo menos uma vez a cada 12 meses.	
O status de conformidade do PCI DSS dos TPSPs é verificado periodicamente.		
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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** É importante que a entidade entenda quais requisitos e sub-requisitos do PCI DSS seus TPSPs concordaram em atender, quais requisitos são compartilhados entre o TPSP e a entidade, e para aqueles que são compartilhados, especificações sobre como os requisitos são compartilhados e qual entidade é responsável por atender a cada sub-requisito. Sem esse entendimento compartilhado, é inevitável que a entidade e o TPSP assumam que um determinado sub-requisito do PCI DSS é de responsabilidade da outra parte e, portanto, esse sub-requisito pode não ser atendido de forma alguma. As informações específicas que uma entidade mantém dependerá do acordo específico com seus fornecedores, o tipo de serviço, etc. Os TPSPs podem definir suas responsabilidades de PCI DSS como sendo as mesmas para todos os seus clientes; caso contrário, essa responsabilidade deve ser acordada entre a entidade e o TPSP. **Práticas Recomendadas** As entidades podem documentar essas responsabilidades por meio de uma matriz que identifica todos os requisitos aplicáveis do PCI DSS e indica para cada requisito se a entidade ou o TPSP é responsável por atender a esse requisito ou se é uma responsabilidade compartilhada. Esse tipo de documento costuma ser chamado de *matriz de responsabilidade.* *(continua na página a seguir)*
12.8.5 São mantidas informações sobre quais requisitos do PCI DSS são gerenciados por cada TPSP, quais são gerenciados pela entidade e quaisquer que sejam compartilhados entre o TPSP e a entidade.	**12.8.5.a** Examine as políticas e procedimentos para verificar se os processos são definidos para manter informações sobre quais requisitos do PCI DSS são gerenciados por cada TPSP, quais são gerenciados pela entidade e quaisquer que sejam compartilhados entre o TPSP e a entidade.	
	12.8.5.b Examine a documentação e entreviste a equipe para verificar se a entidade mantém informações sobre quais requisitos do PCI DSS são gerenciados por cada TPSP, quais são gerenciados pela entidade e quaisquer que sejam compartilhados entre as duas entidades.	
Objetivo da Abordagem Personalizada		
Os registros detalhando os requisitos do PCI DSS e os componentes de sistema relacionados pelos quais cada TPSPs é única ou conjuntamente responsável, são mantidos e revisados periodicamente.		

Requisitos e Procedimentos de Teste		Diretriz
		Também é importante que as entidades entendam se quaisquer TPSPs tem relacionamentos “aninhados” com outros TPSPs, o que significa que os contratos de TPSP primários com outro(s) TPSP(s) para fins de prestação de um serviço. É importante entender se o TPSP primário está contando com o(s) TPSP(s) secundário(s) para alcançar a conformidade geral de um serviço e como o TPSP primário está monitorando o desempenho do serviço e o status de conformidade do PCI DSS do(s) TPSP(s) secundário(s). Observe que é responsabilidade do TPSP primário gerenciar e monitorar quaisquer TPSPs secundários. **Informações Adicionais** Consulte o *Suplemento de Informações: Garantia de Segurança de Terceiros* para um amostra do modelo de matriz de responsabilidade.

Requisitos e Procedimentos de Teste		Diretriz
12.9 Os prestadores de serviços terceirizados (TPSPs) oferecem suporte à conformidade com o PCI DSS de seus clientes.		
Requisitos da Abordagem Definida **12.9.1** ***Requisito adicional apenas para prestadores de serviços:*** Os TPSPs reconhecem por escrito aos clientes que são responsáveis pela segurança dos dados da conta que o TPSP possui ou armazena, processa ou transmite em nome do cliente, ou na medida em que possam impactar a segurança do CDE do cliente. **Objetivo da Abordagem Personalizada** Os TPSPs reconhecem formalmente suas responsabilidades de segurança para com seus clientes. **Observações de Aplicabilidade** Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços. A redação exata de um reconhecimento dependerá do acordo entre as duas partes, dos detalhes do serviço prestado e das responsabilidades atribuídas a cada uma das partes. O reconhecimento não precisa incluir a redação exata fornecida neste requisito.	**Procedimentos de Teste da Abordagem Definida** **12.9.1** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as políticas, procedimentos e modelos usados pelo TPSP para acordos escritos para verificar se os processos são definidos para o TPSP fornecer reconhecimentos por escrito aos clientes de acordo com todos os elementos especificados neste requisito.	**Objetivo** Em conjunto com o Requisito 12.8.2, este requisito visa promover um nível consistente de entendimento entre os TPSPs e seus clientes sobre as responsabilidades aplicáveis do PCI DSS. O reconhecimento dos TPSPs evidencia seu compromisso em manter a segurança adequada dos dados da conta que obtém de seus clientes. O método pelo qual o TPSP fornece confirmação por escrito deve ser acordado entre o prestador e seus clientes.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.9.2 ***Requisito adicional apenas para prestadores de serviços:*** Os TPSPs apoiam as solicitações de informações de seus clientes para atender aos Requisitos 12.8.4 e 12.8.5, fornecendo o seguinte mediante solicitação do cliente: • Informações de status de conformidade do PCI DSS para qualquer serviço que o TPSP executa em nome dos clientes (Requisito 12.8.4). • Informações sobre quais requisitos PCI DSS são de responsabilidade do TPSP e quais são de responsabilidade do cliente, incluindo quaisquer responsabilidades compartilhadas (Requisito 12.8.5).	**12.9.2** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as políticas e procedimentos para verificar se os processos são definidos para os TPSPs para apoiar a solicitação dos clientes por informações para atender aos Requisitos 12.8.4 e 12.8.5 de acordo com todos os elementos especificados neste requisito.	Se um TPSP não fornecer as informações necessárias para permitir que seus clientes atendam aos requisitos de segurança e conformidade, os clientes não poderão proteger os dados do titular do cartão nem cumprir suas próprias obrigações contratuais. **Práticas Recomendadas** Se um TPSP tiver um Atestado de Conformidade do PCI DSS (AOC), a expectativa é que o TPSP forneça isso aos clientes, mediante solicitação, para demonstrar seu status de conformidade com o PCI DSS. Se o TPSP não passou por uma avaliação do PCI DSS, eles podem fornecer outras evidências suficientes para demonstrar que atendeu aos requisitos aplicáveis sem passar por uma validação de conformidade formal. Por exemplo, o TPSP pode fornecer evidências específicas ao assessor da entidade para que o assessor possa confirmar que os requisitos aplicáveis foram atendidos. Alternativamente, o TPSP pode optar por se submeter a várias avaliações sob demanda por cada um dos assessores de seus clientes, com cada avaliação direcionada para confirmar se os requisitos aplicáveis sejam atendidos. Os TPSPs devem fornecer evidências suficientes aos seus clientes para verificar se o escopo da avaliação do PCI DSS do TPSP abrangeu os serviços aplicáveis ao cliente e se os requisitos relevantes do PCI DSS foram examinados e determinados como estando implementados. *(continua na página a seguir)*
Objetivo da Abordagem Personalizada		
Os TPSPs fornecem informações conforme necessário para apoiar os esforços de conformidade de seus clientes com o PCI DSS.		
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

Requisitos e Procedimentos de Teste		Diretriz
		Os TPSPs podem definir suas responsabilidades de PCI DSS como sendo as mesmas para todos os seus clientes; caso contrário, essa responsabilidade deve ser acordada entre o cliente e a TPSP. É importante que o cliente compreenda quais requisitos e sub-requisitos do PCI DSS seus TPSPs concordaram em atender, quais requisitos são compartilhados entre o TPSP e o cliente, e para aqueles que são compartilhados, especificações sobre como os requisitos são compartilhados e qual entidade é responsável por atender a cada sub-requisito. Um exemplo de uma maneira de documentar essas responsabilidades é por meio de uma matriz que identifica todos os requisitos aplicáveis do PCI DSS e indica se o cliente ou TPSP é responsável por atender a esse requisito ou se é uma responsabilidade compartilhada. **Informações Adicionais** Para obter mais orientações, consulte: • Seção PCI DSS: *Uso de Prestadores de Serviço Terceirizados*. • *Suplemento de Informações: Garantia de Segurança de Terceiros* (inclui uma amostra do modelo de matriz de responsabilidade)

Requisitos e Procedimentos de Teste		Diretriz
12.10 Incidentes de segurança suspeitos e confirmados que poderiam impactar o CDE são respondidos imediatamente.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
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 legais para reportar comprometimentos. • Cobertura e respostas de todos os componentes críticos de sistema. • Referência ou inclusão de procedimentos de resposta a incidentes das bandeiras de pagamento.	**12.10.1.a** Examine o plano de resposta a incidentes para verificar se o plano existe e inclui pelo menos os elementos especificados neste requisito. **12.10.1.b** Entreviste o pessoal e examine a documentação de incidentes ou alertas relatados anteriormente para verificar se o plano de resposta a incidentes documentado e os procedimentos foram seguidos.	**Objetivo** Sem um plano abrangente de resposta a incidentes que seja devidamente disseminado, lido e compreendido pelas partes responsáveis, a confusão e a falta de uma resposta unificada podem criar mais tempo de inatividade para a empresa, exposição desnecessária na mídia pública, bem como risco financeiro e/ou de perda da reputação e responsabilidades legais. **Práticas Recomendadas** O plano de resposta a incidentes deve ser completo e conter todos os elementos primordiais para as partes interessadas (por exemplo, jurídico, comunicações) para permitir que a entidade responda de forma eficaz no caso de uma violação que possa impactar os dados da conta. É importante manter o plano atualizado com informações de contato atualizadas de todos os indivíduos designados como tendo uma função na resposta a incidentes. Outras partes relevantes para notificações podem incluir clientes, instituições financeiras (adquirentes e emissores) e parceiros de negócios. As entidades devem considerar como abordar todos os comprometimentos de dados dentro do CDE em seus planos de resposta a incidentes, incluindo dados da conta, chaves de criptografia wireless, chaves de criptografia usadas para transmissão e armazenamento ou dados da conta ou dados do titular do cartão, etc. **Exemplos** Os requisitos legais para reportar comprometimentos incluem aqueles na maioria dos estados dos EUA, o General Data Protection Regulation (GDPR) da União Europeia, e a Personal Data Protection Act (Cingapura). *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Um plano abrangente de resposta a incidentes que atenda às expectativas da bandeira do cartão é mantido.		**Informações Adicionais** Para obter mais informações, consulte o *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Requisitos da Abordagem Definida **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.	**Procedimentos de Teste da Abordagem Definida** **12.10.2** Entreviste a equipe e Examine a documentação para verificar se, pelo menos uma vez a cada 12 meses, o plano de resposta a incidentes de segurança está: • Revisado e atualizado conforme necessário. • Testado, incluindo todos os elementos listados no Requisito 12.10.1.	**Objetivo** O teste adequado do plano de resposta a incidentes de segurança pode identificar processos de negócios interrompidos e garantir que etapas importantes não sejam perdidas, o que pode resultar em maior exposição durante um incidente. Os testes periódicos do plano garantem que os processos permaneçam viáveis, bem como garantem que todo o pessoal relevante na organização esteja familiarizado com o plano. **Práticas Recomendadas** O teste do plano de resposta a incidentes pode incluir incidentes simulados e as respostas correspondentes na forma de um “exercício de mesa”, que inclui a participação do pessoal relevante. Uma revisão do incidente e da qualidade da resposta pode fornecer às entidades a garantia de que todos os elementos necessários estão incluídos no plano.
Objetivo da Abordagem Personalizada O plano de resposta a incidentes é mantido atualizado e testado periodicamente.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **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. **Objetivo da Abordagem Personalizada** Os incidentes são respondidos imediatamente, quando apropriado.	**Procedimentos de Teste da Abordagem Definida** **12.10.3** Examine a documentação e entreviste o pessoal responsável que ocupa as funções designadas para verificar se o pessoal específico está designado para estar disponível 24 horas por dia, 7 dias por semana, para responder a incidentes de segurança.	**Objetivo** Um incidente pode ocorrer a qualquer momento, portanto, se uma pessoa treinada em resposta a incidentes e familiarizada com o plano da entidade estiver disponível quando um incidente for detectado, a capacidade da entidade de responder corretamente ao incidente é aumentada. **Práticas Recomendadas** Frequentemente, pessoal específico é designado para fazer parte de uma equipe de resposta a incidentes de segurança, com a equipe tendo a responsabilidade geral de responder aos incidentes (talvez em uma base de programação rotativa) e gerenciar esses incidentes de acordo com o plano. A equipe de resposta a incidentes pode consistir em membros centrais que são permanentemente designados ou funcionários “sob demanda” que podem ser chamados conforme necessário, dependendo de sua experiência e das especificações do incidente. Ter recursos disponíveis para responder rapidamente a incidentes minimiza a interrupção da organização. Exemplos de tipos de atividades que a equipe ou indivíduos devem responder incluem qualquer evidência de atividade não autorizada, detecção de pontos de acesso wireless não autorizados, alertas críticos do IDS e relatórios de sistema crítico não autorizado ou alterações de conteúdo de arquivo.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **12.10.4** O pessoal responsável por responder a incidentes de segurança suspeitos e confirmados é adequada e periodicamente treinado em suas responsabilidades de resposta a incidentes.	**Procedimentos de Teste da Abordagem Definida** **12.10.4** Examine a documentação de treinamento e entreviste o pessoal de resposta a incidentes para verificar se o pessoal está devidamente e periodicamente treinado em suas responsabilidades de resposta a incidentes.	**Objetivo** Sem uma equipe de resposta a incidentes treinada e prontamente disponível, danos extensos à rede podem ocorrer e dados e sistemas críticos podem se tornar "poluídos" pelo manuseio inadequado dos sistemas visados. Isso pode impedir o sucesso de uma investigação pós-incidente. **Práticas Recomendadas** É importante que todo o pessoal envolvido na resposta a incidentes seja treinado e tenha conhecimento sobre o gerenciamento de evidências para perícias e investigações.
Objetivo da Abordagem Personalizada Os funcionários estão bem informados sobre seu papel e responsabilidades na resposta a incidentes e podem acessar assistência e orientação quando necessário.		
Requisitos da Abordagem Definida **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.	**Procedimentos de Teste da Abordagem Definida** **12.10.4.1.a** Examine a análise de risco direcionada da entidade para a frequência de treinamento do pessoal de resposta a incidentes para verificar se a análise de risco foi realizada de acordo com todos os elementos especificados no Requisito 12.3.1. **12.10.4.1.b** Examine os resultados documentados do treinamento periódico do pessoal de resposta a incidentes e entreviste o pessoal para verificar se o treinamento é realizado na frequência definida na análise de risco direcionada da entidade realizada para este requisito.	**Objetivo** O ambiente de cada entidade e o plano de resposta a incidentes são diferentes e a abordagem dependerá de uma série de fatores, incluindo o tamanho e a complexidade da entidade, o grau de mudança no ambiente, o tamanho da equipe de resposta a incidentes e a rotatividade de pessoal. A realização de uma análise de risco permitirá que a entidade determine a frequência ideal para o treinamento de pessoal com responsabilidades de resposta a incidentes.
Objetivo da Abordagem Personalizada O pessoal de resposta a incidentes é treinado com uma frequência que aborda o risco da entidade.		
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.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
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 mudanças para arquivos críticos. • O mecanismo de detecção de mudanças 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.	**12.10.5** Examine a documentação e observe os processos de resposta a incidentes para verificar se o monitoramento e a resposta aos alertas dos sistemas de monitoramento de segurança estão incluídos no plano de resposta a incidentes de segurança, incluindo, mas não se limitando aos sistemas especificados neste requisito.	Responder a alertas gerados por sistemas de monitoramento de segurança que são explicitamente projetados para enfocar o risco potencial aos dados é fundamental para evitar uma violação e, portanto, deve ser incluído nos processos de resposta a incidentes.
Objetivo da Abordagem Personalizada		
Os alertas gerados por tecnologias de monitoramento e detecção são respondidos de maneira estruturada e repetível.		
Observações de Aplicabilidade		
O marcador acima (para monitorar e responder a alertas de um mecanismo de detecção de mudanças 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.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Incorporar as lições aprendidas no plano de resposta a incidentes após a ocorrência de um incidente e em sintonia com os desenvolvimentos da indústria ajuda a manter o plano atualizado e capaz de reagir a ameaças emergentes e tendências de segurança. **Práticas Recomendadas** O exercício de lições aprendidas deve incluir todos os níveis de pessoal. Embora muitas vezes seja incluído como parte da revisão de todo o incidente, ele deve se concentrar em como a resposta da entidade ao incidente pode ser melhorada. É importante não apenas considerar os elementos da resposta que não tiveram os resultados planejados, mas também entender o que funcionou bem e se as lições desses elementos que funcionaram bem podem ser aplicadas em áreas do plano que não funcionaram. Outra maneira de otimizar o plano de resposta a incidentes de uma entidade é entender os ataques feitos contra outras organizações e usar essas informações para ajustar os procedimentos de detecção, contenção, mitigação ou recuperação da entidade.
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.	**12.10.6.a** Examine as políticas e procedimentos para verificar se os processos estão definidos para modificar e desenvolver o plano de resposta a incidentes de segurança de acordo com as lições aprendidas e para incorporar os desenvolvimentos da indústria.	
	12.10.6.b Examine o plano de resposta a incidentes de segurança e entreviste o pessoal responsável para verificar se o plano de resposta a incidentes foi modificado e evoluído de acordo com as lições aprendidas e para incorporar os desenvolvimentos da indústria.	
Objetivo da Abordagem Personalizada		
A eficácia e a precisão do plano de resposta a incidentes são revisadas e atualizadas após cada invocação.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
12.10.7 Os procedimentos de resposta a incidentes estão implementados, 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. • Corrigir o vazamentos de dados ou lacunas de processo que resultaram nos dados da conta onde não eram esperados.	**12.10.7.a** Examine os procedimentos documentados de resposta a incidentes para verificar se os procedimentos para responder à detecção do PAN armazenado em qualquer lugar onde não se espera que exista estão prontos para serem iniciados e incluem todos os elementos especificados neste requisito.	Ter procedimentos documentados de resposta a incidentes que são seguidos caso o PAN armazenado seja encontrado em qualquer lugar onde não se espera ajuda a identificar as ações de remediação necessárias e evitar vazamentos futuros. **Práticas Recomendadas** Se o PAN for encontrado fora do CDE, a análise deve ser realizada para 1) determinar se ele foi salvo independentemente de outros dados ou com dados de autenticação confidenciais, 2) identificar a fonte dos dados e 3) identificar as lacunas de controle que resultaram no dados fora do CDE. As entidades devem considerar se existem fatores contributivos, como processos de negócios, comportamento do usuário, configurações inadequadas do sistema, etc. que fizeram com que o PAN fosse armazenado em um local inesperado. Se tais fatores contribuintes estiverem presentes, eles devem ser tratados de acordo com este requisito para prevenir a recorrência.
Objetivo da Abordagem Personalizada	**12.10.7.b** Entreviste a equipe e examine os registros das ações de resposta para verificar se os procedimentos de resposta a incidentes são realizados após a detecção do PAN armazenado em qualquer lugar onde não seja esperado.	
Os processos estão em vigor para responder, analisar e resolver rapidamente as situações, caso o PAN em texto não criptografado seja detectado onde não é esperado.		
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

Este apêndice contém requisitos adicionais do PCI DSS para diferentes tipos de entidades. As seções deste Apêndice incluem:

- Apêndice A1: Requisitos Adicionais do PCI DSS para Prestadores de Serviços Multilocatários.
- Apêndice A2: Requisitos Adicionais do PCI DSS para Entidades que usam SSL/TLS Antigo para Conexões de Terminal POS POI com Cartão Presente.
- Apêndice A3: Validação Complementar de Entidades Designadas (DESV).

Informações de orientação e aplicabilidade são fornecidas em cada seção.

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

Seções
A1.1 Os prestadores de serviços multilocatários protegem e separam todos os ambientes e dados do cliente.
A1.2 Os prestadores de serviços multilocatários facilitam o registro e a resposta a incidentes para todos os clientes.

Visão Geral
Todos os prestadores de serviços são responsáveis por atender aos requisitos do PCI DSS para seus próprios ambientes, conforme aplicável aos serviços oferecidos a seus clientes. Além disso, os prestadores de serviços multilocatários devem atender aos requisitos deste Apêndice.
Os prestadores de serviços multilocatários são um tipo de prestadores de serviço terceirizados que oferecem vários serviços compartilhados para comerciantes e outros prestadores de serviços, nos quais os clientes compartilham os recursos do sistema (tais como um servidor físico ou virtual), infraestrutura, aplicativos (incluindo Software como um Serviço (SaaS)), e/ou bancos de dados. Os serviços podem incluir, mas não se limitando a, hospedar várias entidades em um único servidor compartilhado, fornecer serviços de comércio eletrônico e/ou "carrinho de compras", serviços de hospedagem baseados na web, aplicativos de pagamento, vários aplicativos e serviços em nuvem e conexões para gateways de pagamento e processadores.
Os prestadores de serviços que fornecem apenas serviços de data center compartilhados (muitas vezes chamados de provedores de co-locação ou "co-lo"), onde o equipamento, espaço e largura de banda estão disponíveis para aluguel, não são considerados prestadores de serviços multilocatário para os fins deste Apêndice.
Observação: Mesmo que um prestador de serviços multilocatário possa atender a esses requisitos, cada cliente ainda é responsável por cumprir os requisitos do PCI DSS aplicáveis ao seu ambiente e validar a conformidade conforme aplicável. Frequentemente, existem requisitos do PCI DSS para os quais a responsabilidade é compartilhada entre o fornecedor e o cliente (talvez para diferentes aspectos do ambiente). Os requisitos 12.8 e 12.9 delineiam os requisitos específicos para os relacionamentos entre todos os prestadores de serviços terceirizados (TPSPs) e seus clientes, e as responsabilidades de ambos. Isso inclui a definição dos serviços específicos que o cliente está recebendo, juntamente com os requisitos do PCI DSS que são de responsabilidade do cliente atender, quais são da responsabilidade do TPSP e quais requisitos são compartilhados entre o cliente e o TPSP.

Requisitos e Procedimentos de Teste		Diretriz
A1.1 Os prestadores de serviços multilocatários protegem e separam todos os ambientes e dados do cliente.		
Requisitos da Abordagem Definida **A1.1.1** A separação lógica é implementada da seguinte forma: • O provedor não pode acessar os ambientes de seus clientes sem autorização. • Os clientes não podem acessar o ambiente do provedor sem autorização. **Objetivo da Abordagem Personalizada** Os clientes não podem acessar o ambiente do provedor. O provedor não pode acessar os ambientes de seus clientes sem autorização. **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.*	**Procedimentos de Teste da Abordagem Definida** **A1.1.1** Examine a documentação e as configurações do sistema e da rede e entreviste o pessoal para verificar se a separação lógica está implementada de acordo com todos os elementos especificados neste requisito.	**Objetivo** Sem controles entre o ambiente do fornecedor e o ambiente do cliente, um agente malicioso dentro do ambiente do fornecedor pode comprometer o ambiente do cliente e, da mesma forma, um agente malicioso no ambiente do cliente pode comprometer o fornecedor e potencialmente outros clientes do provedor. Ambientes multilocatários devem ser isolados uns dos outros e da infraestrutura do provedor, de modo que possam ser entidades gerenciadas separadamente sem conectividade entre eles. **Práticas Recomendadas** Os provedores devem garantir uma forte separação entre os ambientes projetados para o acesso do cliente, por exemplo, portais de configuração e cobrança, e o ambiente privado do provedor, que só deve ser acessado por pessoal autorizado do provedor. O acesso do prestador de serviços aos ambientes do cliente é realizado de acordo com o requisito 8.2.3. **Informações Adicionais** Consulte o *Suplemento de Informações: Diretrizes de Computação em Nuvem do PCI SSC* para obter mais orientações sobre ambientes em nuvem.

<table>
<tr><th colspan="2">Requisitos e Procedimentos de Teste</th><th>Diretriz</th></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="3">Objetivo
É importante que um prestador de serviços multilocatário defina controles para que cada cliente só possa acessar seu próprio ambiente e CDE para evitar o acesso não autorizado de um ambiente de cliente a outro.
Exemplos
Em uma infraestrutura baseada em nuvem, como uma oferta de infraestrutura como serviço (IaaS), o CDE dos clientes pode incluir dispositivos de rede virtuais e servidores virtuais que são configurados e gerenciados pelos clientes, incluindo sistemas operacionais, arquivos, memória, etc.</td></tr>
<tr><td rowspan="2">A1.1.2 Os controles são implementados de forma que cada cliente só tenha permissão para acessar seus próprios dados do titular do cartão e CDE.

Objetivo da Abordagem Personalizada
Os clientes não podem acessar os ambientes de outros clientes.</td><td>A1.1.2.a Examine a documentação para verificar se os controles estão definidos de forma que cada cliente só tenha permissão para acessar seus próprios dados do titular do cartão e CDE.</td></tr>
<tr><td>A1.1.2.b Examine as configurações do sistema para verificar se os clientes têm privilégios estabelecidos para acessar apenas seus próprios dados da conta e CDE.</td></tr>
<tr><td>Requisitos da Abordagem Definida</td><td>Procedimentos de Teste da Abordagem Definida</td><td rowspan="2">Objetivo
Para evitar qualquer impacto inadvertido ou intencional nos ambientes de outros clientes ou nos dados da conta, é importante que cada cliente possa acessar apenas os recursos alocados para esse cliente.</td></tr>
<tr><td>A1.1.3 Os controles são implementados de forma que cada cliente possa acessar apenas os recursos alocados a eles.

Objetivo da Abordagem Personalizada
Os clientes não podem afetar os recursos alocados a outros clientes.</td><td>A1.1.3 Examine os privilégios do cliente para verificar se cada cliente pode acessar apenas os recursos alocados a eles.</td></tr>
</table>

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **A1.1.4** A eficácia dos controles de separação lógica usados para separar os ambientes do cliente é confirmada pelo menos uma vez a cada seis meses por meio de testes de penetração. **Objetivo da Abordagem Personalizada** A segmentação dos ambientes do cliente de outros ambientes é validada periodicamente para ser eficaz. **Observações de Aplicabilidade** O teste de separação adequada entre clientes em um ambiente de prestador de serviços multilocatário é um acréscimo aos testes de penetração especificados no Requisito 11.4.6 *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.*	**Procedimentos de Teste da Abordagem Definida** **A1.1.4** Examine os testes de penetração mais recente para verificar se o teste confirmou a eficácia dos controles de separação lógica usados para separar os ambientes do cliente.	**Objetivo** Os prestadores de serviços multilocatários são responsáveis por gerenciar a segmentação entre seus clientes. Sem a garantia técnica de que os controles de segmentação são eficazes, é possível que mudanças na tecnologia do prestador de serviços criem inadvertidamente uma vulnerabilidade que pode ser explorada em todos os clientes do prestador de serviços. **Práticas Recomendadas** A eficácia das técnicas de separação pode ser confirmada usando ambientes temporários (mock-up) criados pelo prestador de serviços que representam os ambientes do cliente e tentando 1) acessar um ambiente temporário de outro ambiente e 2) acessar um ambiente temporário da Internet.

Requisitos e Procedimentos de Teste		Diretriz
A1.2 Os prestadores de serviços multilocatários facilitam o registro e a resposta a incidentes para todos os clientes.		
Requisitos da Abordagem Definida **A1.2.1** O recurso de registro de auditoria é habilitado para cada ambiente do cliente que seja consistente com o Requisito 10 do PCI DSS, incluindo: • Os registros são habilitados para aplicativos comuns de terceiros. • Os registros estão ativos por padrão. • Os registros estão disponíveis para revisão apenas pelo cliente proprietário. • Os locais dos registros são claramente comunicados ao cliente proprietário. • Os dados de registro e a disponibilidade são consistentes com o Requisito 10 do PCI DSS. **Objetivo da Abordagem Personalizada** O recurso de registro está disponível para todos os clientes sem afetar a confidencialidade de outros clientes.	**Procedimentos de Teste da Abordagem Definida** **A1.2.1** Examine a documentação e as definições de configuração do sistema para verificar se o provedor habilitou o recurso de registro de auditoria para cada ambiente do cliente de acordo com todos os elementos especificados neste requisito.	**Objetivo** As informações de registro são úteis para detectar e solucionar problemas de incidentes de segurança e são inestimáveis para investigações forenses. Os clientes, portanto, precisam ter acesso a esses registros. Não obstante, as informações de registro também podem ser usadas por um atacante para reconhecimento e, portanto, as informações de registro de um cliente só podem ser acessadas pelo cliente ao qual o registro está relacionado.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** No caso de uma violação suspeita ou confirmada de confidencialidade dos dados do titular do cartão, o investigador forense de um cliente visa encontrar a causa da violação, excluir o atacante do ambiente e garantir que todo o acesso não autorizado seja removido. Respostas rápidas e eficientes às solicitações dos investigadores forenses podem reduzir significativamente o tempo que o investigador leva para proteger o ambiente do cliente.
A1.2.2 Processos ou mecanismos são implementados para apoiar e/ou facilitar investigações forenses imediatas no caso de um incidente de segurança suspeito ou confirmado para qualquer cliente.	**A1.2.2** Examine os procedimentos documentados para verificar se o provedor tem processos ou mecanismos para apoiar e/ou facilitar uma investigação forense imediata de servidores relacionados no caso de um incidente de segurança suspeito ou confirmado para qualquer cliente.	
Objetivo da Abordagem Personalizada		
A investigação forense está prontamente disponível para todos os clientes em caso de suspeita ou confirmação de um incidente de segurança.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **A1.2.3** Processos ou mecanismos são implementados para relatar e abordar incidentes de segurança suspeitos ou confirmados e vulnerabilidades, incluindo: • Os clientes podem relatar incidentes de segurança e vulnerabilidades ao provedor com segurança. • O prestador aborda e corrige incidentes de segurança suspeitos ou confirmados e vulnerabilidades de acordo com o Requisito 6.3.1. **Objetivo da Abordagem Personalizada** Incidentes ou vulnerabilidades de segurança suspeitos ou confirmados são descobertos e resolvidos. Os clientes são informados quando apropriado. **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.*	**Procedimentos de Teste da Abordagem Definida** **A1.2.3** Examine os procedimentos documentados e entreviste o pessoal para verificar se o prestador tem um mecanismo para relatar e tratar incidentes de segurança suspeitos ou confirmados e vulnerabilidades, de acordo com todos os elementos especificados neste requisito.	**Objetivo** Vulnerabilidades de segurança nos serviços prestados podem impactar a segurança de todos os clientes do prestador de serviço e, portanto, devem ser gerenciadas de acordo com os processos estabelecidos pelo prestador de serviço, com prioridade para resolver vulnerabilidades que tenham a maior probabilidade de comprometimento. Os clientes provavelmente notarão vulnerabilidades e configurações incorretas de segurança ao usar o serviço. A implementação de métodos seguros para que os clientes relatem incidentes e vulnerabilidades de segurança incentiva os clientes a relatar problemas em potencial e permite que o provedor aprenda rapidamente e resolva problemas em potencial em seu ambiente.

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

Seções

A2.1 Terminais POI usando SSL e/ou TLS antigo são confirmados como não suscetíveis a explorações de SSL/TLS conhecidas.

Visão Geral

Este Apêndice se aplica apenas a entidades que usam SSL/TLS antigo como um controle de segurança para proteger terminais POS POI, incluindo prestadores de serviços que fornecem conexões em terminais POS POI.

As entidades que usam SSL e TLS antigo para conexões de terminal POS POI devem trabalhar para atualizar para um protocolo criptográfico forte o mais rápido possível. Além disso, SSL e/ou TLS antigo não devem ser introduzidos em ambientes onde esses protocolos ainda não existam. No momento da publicação, as vulnerabilidades conhecidas são difíceis de explorar em terminais de pagamento POS POI. Todavia, novas vulnerabilidades podem surgir a qualquer momento e cabe à organização se manter atualizada com as tendências de vulnerabilidade e determinar se ela é suscetível a quaisquer explorações conhecidas.

Os requisitos do PCI DSS diretamente afetados são:

– **Requisito 2.2.5**: Onde houver serviços, protocolos ou daemons inseguros; a justificativa de negócios é documentada e recursos de segurança adicionais são documentados e implementados para reduzir o risco de usar serviços, protocolos ou daemons inseguros.

– **Requisito 2.2.7**: Todo o acesso administrativo fora do console é criptografado usando criptografia forte.

– **Requisito 4.2.1**: Criptografia forte e protocolos de segurança são implementados de forma a proteger o PAN durante a transmissão em redes públicas abertas.

O SSL e TLS antigo não devem ser usados como um controle de segurança para atender a esses requisitos, exceto no caso de conexões de terminal POS POI, conforme detalhado neste apêndice. Para apoiar as entidades que trabalham para migrar de SSL /TLS antigo em terminais POS POI, as seguintes disposições estão incluídas:

- As novas implementações de terminal POS POI não devem usar SSL ou TLS antigo como um controle de segurança.
- Todos os prestadores de serviços de terminal POS POI devem fornecer uma oferta de serviço segura.
- Os prestadores de serviços que suportam as implementações de terminais POS POI existentes que usam SSL e/ou TLS antigo devem ter um plano de migração e mitigação de risco formal em vigor.
- Os terminais POS POI em ambientes com cartão presente que podem ser verificados como não sendo suscetíveis a quaisquer explorações conhecidas de SSL e TLS antigo, **e os pontos de terminação SSL/TLS aos quais se conectam**, podem continuar usando SSL/TLS antigo como um controle de segurança.

Os requisitos neste Apêndice não são elegíveis para a Abordagem Personalizada.

Requisitos e Procedimentos de Teste		Diretriz
A2.1 Terminais POI usando SSL e/ou TLS antigo são confirmados não suscetíveis a explorações de SSL/TLS conhecidas.		
Requisitos da Abordagem Definida **A2.1.1** Quando os terminais POS POI no estabelecimento ou local de aceitação de pagamento usam SSL e/ou TLS antigo, a entidade confirma que os dispositivos não são suscetíveis a quaisquer explorações conhecidas para esses protocolos. **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas. **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 serviços 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 POS POI. A permissão para terminais POS POI que não são atualmente suscetíveis a explorações é baseada nos riscos atualmente conhecidos. Se forem introduzidos novos *exploits* aos quais os terminais POS POI são suscetíveis, os terminais POS POI precisarão ser atualizados imediatamente.	**Procedimentos de Teste da Abordagem Definida** **A2.1.1** Para terminais POS POI usando SSL e/ou TLS antigo, confirme se a entidade possui 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 antigo.	**Objetivo** Os terminais POS POI usados em ambientes com cartão presente podem continuar usando SSL/TLS antigo quando puder ser mostrado que o terminal POS POI não é suscetível às explorações atualmente conhecidos. **Práticas Recomendadas** No entanto, SSL é uma tecnologia desatualizada e pode ser suscetível a vulnerabilidades de segurança adicionais no futuro; portanto, é altamente recomendável que os terminais POS POI sejam atualizados para um protocolo seguro o mais rápido possível. Se SSL/TLS antigo não for necessário no ambiente, o uso e a retorno para essas versões devem ser desabilitados. **Informações Adicionais** Consulte os Suplementos de Informações atuais do PCI SSC sobre SSL/TLS antigo para obter mais orientações.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Os pontos de terminação de POS POI, incluindo, mas não se limitando a prestadores de serviços, como adquirentes ou processadores de adquirentes, podem continuar usando SSL/TLS antigo quando puder ser demonstrado que o prestador de serviços possui controles implementados que mitigam o risco de suportar essas conexões para o ambiente do prestador de serviços. **Práticas Recomendadas** Os prestadores de serviço devem comunicar a todos os clientes que usam SSL/TLS antigo sobre os riscos associados ao seu uso e a necessidade de migrar para um protocolo seguro. **Definições** O plano de migração e de mitigação de risco é um documento preparado pela entidade que detalha seus planos de migração para um protocolo seguro e descreve os controles que a entidade possui para reduzir o risco associado ao SSL/TLS antigo até que a migração seja concluída. **Informações Adicionais** Consulte os Suplementos de Informações atuais do PCI SSC sobre SSL/TLS antigo para obter mais orientações sobre mitigação de riscos e planos de migração.
A2.1.2 ***Requisito adicional apenas para prestadores de serviços:*** Todos os prestadores de serviços com pontos de conexão existentes para terminais POS POI que usam SSL e/ou TLS antigo, conforme definido em A2.1, têm um plano de migração e mitigação de risco formal implementado que inclui: • Descrição de uso, incluindo quais dados estão sendo transmitidos, tipos e número de sistemas que usam e/ou suportam SSL/TLS antigo e tipo de ambiente. • Resultados da avaliação de risco e controles de redução de risco implementados. • Descrição dos processos para monitorar novas vulnerabilidades associadas ao SSL/TLS antigo. • Descrição dos processos de controle de mudança que são implementados para garantir que SSL/TLS antigo não seja implementado em novos ambientes. • Visão geral do plano de projeto de migração para substituir SSL/TLS antigo em uma data futura.	**A2.1.2** ***Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Revise o plano de migração e mitigação de risco documentado para verificar se ele inclui todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada Este requisito não se aplica às abordagens personalizadas.		
Observações de Aplicabilidade Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
A2.1.3 Requisito adicional apenas para prestadores de serviços: Todos os prestadores de serviço fornecem uma oferta de serviço segura.	**A2.1.3 *Procedimento de teste adicional apenas para avaliações de prestadores de serviços:*** Examine as configurações do sistema e a documentação de suporte para verificar se o prestador de serviços oferece uma opção de protocolo seguro para seu serviço.	Os clientes devem ser capazes de optar por atualizar seus POIs para eliminar a vulnerabilidade no uso de SSL e TLS antigo. Em muitos casos, os clientes precisarão adotar uma abordagem em fases ou gradual para migrar seus POS POIs do protocolo inseguro para um protocolo seguro e, portanto, exigirão que o prestador de serviços ofereça suporte a uma oferta segura. **Informações Adicionais** Consulte os Suplementos de Informações atuais do PCI SSC sobre SSL/TLS antigo para obter mais orientações.
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		
Observações de Aplicabilidade		
Estes requisitos se aplicam apenas quando a entidade que está sendo avaliada é um prestador de serviços.		

Apêndice A3: Validação Complementar de Entidades Designadas (DESV)

Seções
A3.1 Um programa de conformidade com o PCI DSS é implementado.
A3.2 O escopo do PCI DSS é documentado e validado.
A3.3 O PCI DSS é incorporado às atividades de negócios habituais (BAU).
A3.4 O acesso lógico ao ambiente de dados do titular do cartão é controlado e gerenciado.
A3.5 Eventos suspeitos são identificados e respondidos.

Visão Geral

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. Uma entidade é obrigada a passar por uma avaliação de acordo com este Apêndice SOMENTE se instruída a fazê-lo por um adquirente ou uma bandeira de pagamento. Exemplos de entidades às quais este Apêndice pode se aplicar incluem:

- Aqueles que armazenam, processam e/ou transmitem grandes volumes de dados da conta,
- Aqueles que fornecem pontos de agregação para dados da conta, ou
- Aqueles que sofreram violações significativas ou repetidas de dados da conta.

Além disso, outros padrões PCI podem fazer referência a completar este Apêndice.

Essas etapas de validação complementares destinam-se a fornecer maior garantia de que os controles do PCI DSS sejam mantidos de forma eficaz e contínua por meio da validação dos processos de negócios habituais (BAU) e maior validação e consideração do escopo.

***Observação**: Alguns requisitos têm prazos definidos (por exemplo, pelo menos uma vez a cada três meses ou pelo menos uma vez a cada seis meses) dentro dos quais certas atividades devem ser realizadas. Para a avaliação inicial deste documento, não é necessário que uma atividade tenha sido realizada para cada período de tempo durante o ano anterior, se o assessor verificar:*

- *A atividade foi realizada de acordo com o requisito aplicável dentro do período de tempo mais recente (por exemplo, o período de três ou seis meses mais recente), e*
- *A entidade documentou políticas e procedimentos para continuar a realizar a atividade dentro do prazo definido.*

Para os anos subsequentes após a avaliação inicial, uma atividade deve ter sido realizada dentro de cada período de tempo exigido (por exemplo, uma atividade exigida a cada três meses deve ter sido realizada pelo menos quatro vezes durante o ano anterior em um intervalo que não exceda 90 dias).

Nem todos os requisitos do PCI DSS se aplicam a todas as entidades que podem passar por uma avaliação do PCI DSS. É por esse motivo que alguns requisitos do PCI DSS estão duplicados neste apêndice. Qualquer dúvida sobre este apêndice deve ser dirigida aos adquirentes ou bandeiras de pagamento.

Requisitos e Procedimentos de Teste		Diretriz
A3.1 Um programa de conformidade com o PCI DSS é implementado.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** A atribuição de gerenciamento executivo das responsabilidades de conformidade do PCI DSS garante a visibilidade de nível executivo do programa de conformidade com o PCI DSS e permite a oportunidade de fazer perguntas apropriadas para determinar a eficácia do programa e influenciar as prioridades estratégicas. **Práticas Recomendadas** A gestão executiva pode incluir cargos de nível C, conselho de administração ou equivalente. Os títulos específicos dependerão da estrutura organizacional específica. A responsabilidade pelo programa de conformidade com o PCI DSS pode ser atribuída a funções individuais e/ou a unidades de negócios dentro da organização.
A3.1.1 A responsabilidade é estabelecida pela gestão executiva para a proteção dos dados da conta e um programa de conformidade do PCI DSS que inclui: • Responsabilidade geral para manter a conformidade com o PCI DSS. • Definindo um estatuto para um programa de conformidade com o PCI DSS. • Fornecer atualizações à gestão executiva e ao conselho de diretores sobre questões e iniciativas de conformidade com o PCI DSS, incluindo atividades de remediação, pelo menos uma vez a cada 12 meses. **Referência do PCI DSS**: *Requisito 12*	**A3.1.1.a** Examine a documentação para verificar se a gestão executiva atribuiu a responsabilidade geral para manter a conformidade com o PCI DSS da entidade. **A3.1.1.b** Examine o estatuto do PCI DSS da empresa para verificar se ele descreve as condições sob as quais o programa de conformidade do PCI DSS é organizado. **A3.1.1.c** Examine a gestão executiva e as atas e/ou apresentações das reuniões da diretoria para garantir que as iniciativas de conformidade com o PCI DSS e as atividades de remediação sejam comunicadas pelo menos uma vez a cada 12 meses.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
A3.1.2 Um programa formal de conformidade com o PCI DSS está implementado que inclui: • Definição de atividades para manter e monitorar a conformidade geral com o PCI DSS, incluindo atividades de negócios habituais. • Processos de avaliação anual do PCI DSS. • Processos para a validação contínua dos requisitos do PCI DSS (por exemplo, diariamente, semanalmente, a cada três meses, conforme aplicável de acordo com o requisito). • Um processo para realizar uma análise de impacto nos negócios para determinar os impactos potenciais do PCI DSS para decisões estratégicas de negócios. **Referência do PCI DSS**: *Requisitos de 1 a 12*	**A3.1.2.a** Examine as políticas e procedimentos de segurança da informação para verificar se os processos estão definidos para um programa formal de conformidade com o PCI DSS que inclui todos os elementos especificados neste requisito. **A3.1.2.b** Entreviste a equipe e observe as atividades de conformidade para verificar se um programa formal de conformidade com o PCI DSS está implementado de acordo com todos os elementos especificados neste requisito.	Um programa formal de conformidade permite que uma organização monitore a integridade de seus controles de segurança, seja proativa se um controle falhar e comunique com eficácia as atividades e o status de conformidade em toda a organização. **Práticas Recomendadas** O programa de conformidade com o PCI DSS pode ser um programa dedicado ou parte de um programa abrangente de conformidade e/ou governança e deve incluir uma metodologia bem definida que demonstra uma avaliação consistente e eficaz. As decisões estratégicas de negócios que devem ser analisadas quanto aos impactos potenciais do PCI DSS podem incluir fusões e aquisições, novas compras de tecnologia ou novos canais de aceitação de pagamento. **Definições** Manter e monitorar a conformidade geral com o PCI DSS de uma organização inclui a identificação de atividades a serem realizadas diariamente, semanalmente, mensalmente, a cada três meses ou anualmente e garantir que essas atividades sejam realizadas de acordo (por exemplo, usando uma autoavaliação de segurança ou metodologia PDCA) . **Exemplos** As metodologias que oferecem suporte ao gerenciamento de programas de conformidade incluem Plan-Do-Check-Act [Planeje - Faça - Verifique - Aja] (PDCA), ISO 27001, COBIT, DMAIC e Six Sigma.
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **A3.1.3** As funções e responsabilidades de conformidade com o PCI DSS são especificamente definidas e formalmente atribuídas a um ou mais funcionários, incluindo: • Gerenciando atividades normais de negócios do PCI DSS. • Gerenciar avaliações anuais do PCI DSS. • Gerenciar a validação contínua dos requisitos do PCI DSS (por exemplo, diariamente, semanalmente, a cada três meses, conforme aplicável de acordo com o requisito). • Gerenciar a análise de impacto nos negócios para determinar os impactos potenciais do PCI DSS para decisões estratégicas de negócios. **Referência do PCI DSS**: *Requisito 12* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.	**Procedimentos de Teste da Abordagem Definida** **A3.1.3.a** Examine as políticas e procedimentos de segurança da informação e entreviste o pessoal para verificar se as funções e responsabilidades de conformidade com o PCI DSS estão especificamente definidas e formalmente atribuídas a um ou mais funcionários de acordo com todos os elementos deste requisito. **A3.1.3.b** Entreviste a equipe responsável e verifique se eles estão familiarizados e desempenham suas responsabilidades de conformidade com o PCI DSS designadas.	**Objetivo** A definição formal de funções e responsabilidades específicas de conformidade com o PCI DSS ajuda a garantir a responsabilidade e o monitoramento dos esforços contínuos de conformidade com o PCI DSS. **Práticas Recomendadas** O domínio deve ser atribuído a indivíduos com autoridade para tomar decisões baseadas em riscos e sobre os quais recai a responsabilidade pela função específica. Os deveres devem ser definidos formalmente e os “donos” devem ser capazes de demonstrar uma compreensão de suas responsabilidades e responsabilidades. As funções de conformidade podem ser atribuídas a um único proprietário ou a vários proprietários para diferentes elementos de requisito.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O pessoal responsável pela conformidade com o PCI DSS tem necessidades de treinamento específicas que excedem as normalmente fornecidas pelo treinamento geral de conscientização de segurança para permitir que desempenhem sua função. **Práticas Recomendadas** Indivíduos com responsabilidades de conformidade com o PCI DSS devem receber treinamento especializado que, além de uma consciência geral de segurança da informação, enfoca tópicos, habilidades, processos ou metodologias de segurança específicos que devem ser seguidos para que esses indivíduos desempenhem suas responsabilidades de conformidade com eficácia. O treinamento pode ser oferecido por terceiros, como o PCI SSC (por exemplo, PCI Awareness, PCIP e ISA), bandeiras de pagamento e adquirentes, ou o treinamento pode ser interno. O conteúdo do treinamento deve ser aplicável à função de trabalho do indivíduo, ser atualizado e incluir as mais recentes ameaças de segurança e/ou a versão do PCI DSS. **Informações Adicionais** Para obter orientações adicionais, consulte o *Suplemento de Informações: Best Practices for Implementing a Security Awareness Program*.
A3.1.4 O treinamento atualizado em PCI DSS e/ou segurança da informação é fornecido pelo menos uma vez a cada 12 meses para o pessoal com responsabilidades de conformidade com o PCI DSS (conforme identificado em A3.1.3). **Referência do PCI DSS**: *Requisito 12*	**A3.1.4.a** Examine as políticas e procedimentos de segurança da informação para verificar se o treinamento em PCI DSS e/ou segurança da informação é necessário pelo menos uma vez a cada 12 meses para cada função com responsabilidades de conformidade com o PCI DSS.	
	A3.1.4.b Entreviste a equipe e examine os certificados de presença ou outros registros para verificar se a equipe com responsabilidade de conformidade com o PCI DSS recebe treinamento atualizado do PCI DSS e/ou similar em segurança de informações pelo menos uma vez a cada 12 meses.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
A3.2 O escopo do PCI DSS é documentado e validado.		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
A3.2.1 O escopo do PCI DSS é documentado e confirmado quanto à precisão pelo menos uma vez a cada três meses e mediante mudanças significativas no ambiente dentro do escopo. No mínimo, a validação do escopo inclui: • Identificar todos os fluxos de dados para os vários estágios de pagamento (por exemplo, autorização, captura, liquidação, estornos e reembolsos) e canais de aceitação (por exemplo, cartão presente, cartão não-presente e comércio eletrônico). • Atualizar todos os diagramas de fluxo de dados de acordo com o 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. • Para quaisquer dados da conta encontrados fora do CDE definido atualmente, 1) exclua-o com segurança, 2) migre-o para o CDE definido atualmente ou 3) expanda o CDE definido atualmente para incluí-lo. • Identificar todos os componentes de 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.	**A3.2.1.a** Examine os resultados documentados das revisões do escopo e entreviste o pessoal para verificar se as revisões são realizadas: • Pelo menos uma vez a cada três meses. • Após mudanças significativas no ambiente dentro do escopo. **A3.2.1.b** Examine os resultados documentados das revisões do escopo que ocorrem pelo menos uma vez a cada três meses para verificar se a validação do escopo inclui todos os elementos especificados neste requisito.	**Objetivo** A validação frequente do escopo do PCI DSS ajuda a garantir que o escopo do PCI DSS permaneça atualizado e alinhado com os objetivos de negócios em constante mudança e, portanto, que os controles de segurança estejam protegendo todos os componentes apropriados de sistema. **Práticas Recomendadas** O escopo preciso envolve a avaliação crítica do CDE e de todos os componentes de sistema conectados para determinar a cobertura necessária para os requisitos do PCI DSS. As atividades de definição do escopo, incluindo uma análise cuidadosa e monitoramento contínuo, ajudam a garantir que os sistemas dentro do escopo sejam devidamente protegidos. Ao documentar a localização dos dados da conta, a entidade pode considerar a criação de uma tabela ou planilha que inclua as seguintes informações: • Armazenamentos de dados (bancos de dados, arquivos, nuvem, etc.), incluindo a finalidade do armazenamento de dados e o período de retenção, • Quais elementos do CHD são armazenados (PAN, data de validade, nome do titular do cartão e/ou quaisquer elementos do SAD antes da conclusão da autorização), • Como os dados são protegidos (tipo de criptografia e força, algoritmo de hash e força, truncamento, tokenização), • Como o acesso aos armazenamentos de dados é registrado, incluindo uma descrição do(s) mecanismo(s) de registro em uso (solução corporativa, nível de aplicativo, nível de sistema operacional etc.).

Requisitos e Procedimentos de Teste		Diretriz
• Identificar todas as conexões para entidades de terceiros com acesso ao CDE. • Confirmar se todos os fluxos de dados identificados, dados da conta, componentes de sistema, controles de segmentação e conexões de terceiros com acesso ao CDE estão incluídos no escopo. **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS, Requisito de 12* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.		Além de sistemas e redes internos, todas as conexões de entidades terceirizadas - por exemplo, parceiros de negócios, entidades que prestam serviços de suporte remoto e outros prestadores de serviços - precisam ser identificadas para determinar a inclusão no escopo do PCI DSS. Uma vez que as conexões dentro do escopo tenham sido identificadas, os controles do PCI DSS aplicáveis podem ser implementados para reduzir o risco de uma conexão de terceiros ser usada para comprometer o CDE de uma entidade. Uma ferramenta ou metodologia de descoberta de dados pode ser usada para facilitar a identificação de todas as fontes e locais de PAN e para procurar PAN que reside em sistemas e redes fora do CDE atualmente definido ou em locais inesperados dentro do CDE definido - por exemplo, em um registro de erro ou arquivo de despejo de memória. Essa abordagem pode ajudar a garantir que locais anteriormente desconhecidos do PAN sejam detectados e que o PAN seja eliminado ou devidamente protegido. Informações Adicionais Consulte o Suplemento de Informações: Orientação para Escopo e Segmentação de Rede do PCI DSS para orientação adicional.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Mudanças em sistemas ou redes podem ter um impacto significativo no escopo do PCI DSS. Por exemplo, mudanças em conjuntos de regras de controle de segurança de rede podem trazer segmentos de rede inteiros para o escopo, ou novos sistemas podem ser adicionados ao CDE que precisam ser protegidos de forma apropriada. Uma avaliação de impacto formal realizada antes de uma mudança dá à entidade a garantia de que a mudança não afetará adversamente a segurança do CDE. **Práticas Recomendadas** Os processos para determinar o impacto potencial que as mudanças nos sistemas e redes podem ter no escopo do PCI DSS de uma entidade podem ser realizados como parte de um programa de conformidade com o PCI DSS dedicado ou podem cair no programa geral de conformidade e ou governança de uma entidade.
A3.2.2 O impacto do escopo do PCI DSS para todas as mudanças em sistemas ou redes é determinado, incluindo adições de novos sistemas e novas conexões de rede. Os processos incluem: • Executar uma avaliação de impacto formal do PCI DSS. • Identificar os requisitos do PCI DSS aplicáveis ao sistema ou rede. • Atualizar o escopo do PCI DSS conforme apropriado. • Assinatura documentada dos resultados da avaliação de impacto pelo pessoal responsável (conforme definido em A3.1.3). **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS; Requisitos 1 - 12*	**A3.2.2** Examine a documentação da mudança e entreviste a equipe para verificar se para cada mudança nos sistemas ou redes o impacto do escopo do PCI DSS é determinado e inclui todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida **A3.2.2.1** Após a conclusão de uma mudança, todos os requisitos relevantes do PCI DSS são confirmados para serem implementados em todos os sistemas e redes novos ou alterados, e a documentação é atualizada conforme aplicável. **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS; Requisitos 1 - 12* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.	**Procedimentos de Teste da Abordagem Definida** **A3.2.2.1** Examine os registros de mudança e as redes/sistemas afetados e entreviste a para verificar se todos os requisitos relevantes do PCI DSS foram confirmados para serem implementados e a documentação atualizada como parte da mudança.	**Objetivo** É importante ter processos para analisar todas as mudanças feitas em sistemas ou redes, para garantir que todos os controles do PCI DSS apropriados sejam aplicados a quaisquer sistemas ou redes adicionados ao ambiente dentro do escopo devido a uma mudança. A incorporação dessa validação nos processos de gerenciamento de mudanças ajuda a garantir que os inventários de dispositivos e os padrões de configuração sejam mantidos atualizados e que os controles de segurança sejam aplicados quando necessário. **Práticas Recomendadas** Um processo de gerenciamento de mudanças deve incluir evidências de que os requisitos do PCI DSS são implementados ou preservados por meio de um processo iterativo. **Exemplos** Os requisitos do PCI DSS que devem ser verificados incluem, mas não estão limitados a: • Os diagramas de rede são atualizados para refletir as mudanças. • Os sistemas são configurados de acordo com os padrões de configuração, com todas as senhas padrão alteradas e serviços desnecessários desabilitados. • Os sistemas são protegidos com os controles necessários - por exemplo, monitoramento de integridade de arquivos, antimalware, patches e registro de auditoria. • Os dados de autenticação confidenciais não são armazenados e todo o armazenamento de dados da conta é documentado e incorporado à política e procedimentos de retenção de dados. *(continua na página a seguir)*

Requisitos e Procedimentos de Teste		Diretriz
		• Novos sistemas são incluídos no processo de varredura de vulnerabilidade trimestral.
Requisitos da Abordagem Definida **A3.2.3** As mudanças na estrutura organizacional resultam em uma revisão formal (interna) do impacto no escopo do PCI DSS e na aplicabilidade dos controles. **Referência do PCI DSS**: *Requisito 12* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.	**Procedimentos de Teste da Abordagem Definida** **A3.2.3** Examine as políticas e procedimentos para verificar se uma mudança na estrutura organizacional resulta em uma revisão formal do impacto no escopo do PCI DSS e na aplicabilidade dos controles.	**Objetivo** A estrutura e a gestão de uma organização definem os requisitos e protocolo para operações eficazes e seguras. Mudanças nessa estrutura podem ter efeitos negativos nos controles e estruturas existentes, realocando ou removendo recursos que antes suportavam os controles do PCI DSS ou herdando novas responsabilidades que podem não ter estabelecido controles implementados. Portanto, é importante revisitar o escopo e os controles do PCI DSS quando houver mudanças na estrutura e no gerenciamento de uma organização para garantir que os controles estejam implementados e ativos. **Exemplos** Mudanças na estrutura organizacional incluem, mas não estão limitadas a, fusões ou aquisições de empresas e mudanças significativas ou realocações de pessoal com responsabilidade pelos controles de segurança.

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O PCI DSS normalmente requer que os controles de segmentação sejam verificados por testes de penetração a cada doze meses. Validar os controles de segmentação com mais frequência provavelmente descobrirá essas falhas antes que elas possam ser exploradas por um atacante que tenta girar lateralmente de uma rede não confiável fora do escopo para o CDE. **Práticas Recomendadas** Embora o requisito especifique que essa validação de escopo seja realizada pelo menos uma vez a cada seis meses e após uma mudança significativa, este exercício deve ser realizado com a maior frequência possível para garantir que permaneça eficaz no isolamento do CDE de outras redes. **Informações Adicionais** Consulte o *Suplemento de Informações: Guia do Teste de Penetração* para diretrizes adicionais.
A3.2.4 Se a segmentação for usada, o escopo do PCI DSS é confirmado da seguinte forma: • De acordo com a metodologia da entidade definida no Requisito 11.4.1. • O teste de penetração é realizado em controles de segmentação pelo menos uma vez a cada seis meses e após quaisquer alterações nos controles/métodos de segmentação. • O teste de penetração abrange todos os controles/métodos de segmentação em uso. • O teste de penetração verifica se os controles/métodos de segmentação são operacionais e eficazes e isola o CDE de todos os sistemas fora do escopo. **Referência do PCI DSS**: *Requisito 11*	**A3.2.4** Examine os resultados do teste de penetração mais recente para verificar se o teste foi conduzido de acordo com todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
A3.2.5 Uma metodologia de descoberta de dados é implementada para: • Confirmar o escopo do PCI DSS. • Localizar todas as fontes e locais do PAN em texto não criptografado pelo menos uma vez a cada três meses e mediante alterações significativas no CDE ou nos processos. • Abordar o potencial do PAN em texto não criptografado residir em sistemas e redes fora do CDE definido atualmente. **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS*	**A3.2.5.a** Examine a metodologia de descoberta de dados documentada para verificar se ela inclui todos os elementos especificados neste requisito. **A3.2.5.b** Examine os resultados dos esforços recentes de descoberta de dados e entreviste a equipe responsável para verificar se a descoberta de dados é realizada pelo menos uma vez a cada três meses e mediante mudanças significativas no CDE ou nos processos.	O PCI DSS exige que, como parte do exercício de definição do escopo, as entidades avaliadas identifiquem e documentem a existência de todos os PAN em texto não criptografado em seus ambientes. Implementar uma metodologia de descoberta de dados que identifica todas as fontes e locais de PAN em texto não criptografado e procura PAN em texto não criptografado em sistemas e redes fora do CDE definido atualmente ou em locais inesperados dentro do CDE definido - por exemplo, em um registro de erro ou arquivo de despejo de memória - ajuda a garantir que locais anteriormente desconhecidos de PAN em texto não criptografado sejam detectados e protegidos de forma adequada. **Exemplos** Um processo de descoberta de dados pode ser realizado por meio de uma variedade de métodos, incluindo, mas não se limitando a 1) software de descoberta de dados disponível comercialmente, 2) um programa de descoberta de dados desenvolvido internamente ou 3) uma pesquisa manual. Uma combinação de metodologias também pode ser usada conforme necessário. Independentemente do método usado, o objetivo do esforço é encontrar todas as fontes e locais do PAN em texto não criptografado (não apenas no CDE definido).
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Um processo para testar a eficácia dos métodos usados para descoberta de dados garante a integridade e a precisão da detecção de dados da conta. **Práticas Recomendadas** Para completar, os componentes de sistema nas redes dentro do escopo e os sistemas nas redes fora do escopo devem ser incluídos no processo de descoberta de dados. O processo de descoberta de dados deve ser eficaz em todos os sistemas operacionais e plataformas em uso. A precisão pode ser testada colocando PANs de teste nos componentes de sistema e formatos de arquivo em uso e confirmando que o método de descoberta de dados detectou os PANs de teste.
A3.2.5.1 Os métodos de descoberta de dados são confirmados da seguinte forma: • A efetividade dos métodos é testada. • Os métodos são capazes de descobrir o PAN em texto não criptografado em todos os tipos de componentes de sistema e formatos de arquivo em uso. • A eficácia dos métodos de descoberta de dados é confirmada pelo menos uma vez a cada 12 meses. **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS*	**A3.2.5.1.a** Entreviste o pessoal e examine a documentação para verificar: • A entidade possui um processo implementado para testar a eficácia dos métodos usados para descoberta de dados. • O processo inclui a verificação de que os métodos são capazes de descobrir PAN em texto não criptografado em todos os tipos de componentes de sistema e formatos de arquivo em uso.	
Objetivo da Abordagem Personalizada	**A3.2.5.1.b** Examine os resultados dos testes de eficácia para verificar se a eficácia dos métodos de descoberta de dados é confirmada pelo menos uma vez a cada 12 meses.	
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Ter procedimentos de resposta documentados que são seguidos caso o PAN em texto não criptografado seja encontrado fora do CDE ajuda a identificar as ações de remediação necessárias e evitar vazamentos futuros. **Práticas Recomendadas** Se o PAN for encontrado fora do CDE, a análise deve ser realizada para 1) determinar se ele foi salvo independentemente de outros dados ou com dados de autenticação confidenciais, 2) identificar a fonte dos dados e 3) identificar as lacunas de controle que resultaram no dados fora do CDE. As entidades devem considerar se fatores contributivos, como processos de negócios, comportamento do usuário, configurações inadequadas do sistema, etc., fizeram com que o PAN fosse armazenado em um local inesperado. Se tais fatores contribuintes estiverem presentes, eles devem ser tratados de acordo com este requisito para prevenir uma recorrência.
A3.2.5.2 Os procedimentos de resposta são implementados para serem iniciados após a detecção de PAN em texto não criptografado fora do CDE para incluir: • Determinar o que fazer se o PAN em texto não criptografado for descoberto fora do CDE, incluindo sua recuperação, exclusão segura e/ou migração para o CDE definido atualmente, conforme aplicável. • Determinar como os dados foram parar fora do CDE. • Corrigir vazamentos de dados ou lacunas de processo que resultaram em dados fora do CDE. • Identificar a fonte dos dados. • Identificar se algum dado de trilha é armazenado com os PANs.	**A3.2.5.2.a** Examine os procedimentos de resposta documentados para verificar se os procedimentos para responder à detecção de PAN em texto não criptografado fora do CDE estão definidos e incluem todos os elementos especificados neste requisito.	
Objetivo da Abordagem Personalizada	**A3.2.5.2.b** Entreviste a equipe e examine os registros das ações de resposta para verificar se as atividades de correção são realizadas quando o PAN em texto não criptografado é detectado fora do CDE.	
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** O uso de mecanismos para detectar e impedir que PANs não autorizados saiam do CDE permite que uma organização detecte e previna situações que podem levar à perda de dados. **Práticas Recomendadas** A cobertura dos mecanismos deve incluir, mas não se limitar a, e-mails, downloads em mídia removível e saída para impressoras. **Exemplos** Os mecanismos para detectar e prevenir a perda não autorizada de PAN em texto não criptografado podem incluir o uso de ferramentas apropriadas, como soluções de prevenção de perda de dados (DLP), bem como processos e procedimentos manuais.
A3.2.6 Mecanismos são implementados para detectar e impedir que PAN em texto não criptografado saia do CDE por meio de um canal, método ou processo não autorizado, incluindo mecanismos que estão: • Executando ativamente. • Configurados para detectar e evitar que o PAN em texto não criptografado saia do CDE por meio de um canal, método ou processo não autorizado. • Gerando registros de auditoria e alertas após a detecção de PAN em texto não criptografado saindo do CDE por meio de um canal, método ou processo não autorizado. **Referência do PCI DSS**: *Escopo dos Requisitos do PCI DSS; Requisito 12*	**A3.2.6.a** Examinar a documentação e observar os mecanismos implementados para verificar se os mecanismos estão de acordo com todos os elementos especificados neste requisito. **A3.2.6.b** Examine os registros e alertas de auditoria e entreviste a equipe responsável para verificar se os alertas são investigados.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
A3.2.6.1 Os procedimentos de resposta são implementados para serem iniciados na detecção de tentativas de remover o PAN em texto não criptografado do CDE por meio de um canal, método ou processo não autorizado. Os procedimentos de resposta incluem: • Procedimentos para a investigação imediata de alertas pelo pessoal responsável. • Procedimentos para corrigir vazamentos de dados ou lacunas de processo, conforme necessário, para evitar qualquer perda de dados. **Referência do PCI DSS**: *Requisito 12*	**A3.2.6.1.a** Examine os procedimentos de resposta documentados para verificar se os procedimentos para responder à tentativa de remoção do PAN em texto não criptografado do CDE por meio de um canal, método ou processo não autorizado incluem todos os elementos especificados neste requisito: • Procedimentos para a investigação imediata de alertas pelo pessoal responsável. • Procedimentos para corrigir vazamentos de dados ou lacunas de processo, conforme necessário, para evitar qualquer perda de dados.	As tentativas de remover o PAN em texto não criptografado por meio de um canal, método ou processo não autorizado podem indicar intenção maliciosa de roubar dados ou podem ser ações de um funcionário autorizado que não tem conhecimento ou simplesmente não segue os métodos adequados. A investigação imediata dessas ocorrências pode identificar onde a correção precisa ser aplicada e fornece informações valiosas para ajudar a entender de onde vêm as ameaças.
Objetivo da Abordagem Personalizada	**A3.2.6.1.b** Entreviste a equipe e examine os registros das ações tomadas quando o PAN em texto não criptografado é detectado saindo do CDE por meio de um canal, método ou processo não autorizado e verifique se as atividades de correção foram realizadas.	
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
A3.3 O PCI DSS é incorporado às atividades de negócios habituais (BAU).		
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	
A3.3.1 Falhas de sistemas críticos de controle de segurança são detectadas, alertadas e tratadas imediatamente, incluindo, mas não se limitando a falha de: • Controles de segurança de rede • IDS/IPS • FIM • Soluções antimalware • Controles de acesso físico • Controles de acesso lógico • Mecanismos de registro de auditoria • Controles de segmentação (se estiverem em uso) • Mecanismos de revisão de registro de auditoria automatizados. Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes. • Ferramentas de revisão de código automático (se estiverem em uso) Este marcador é uma prática recomendada até sua data efetiva; consulte as notas de aplicabilidade abaixo para obter detalhes. **Referência do PCI DSS**: *Requisitos 1 – 12*	**A3.3.1.a** Examine as políticas e procedimentos documentados para verificar se os processos estão definidos para detectar, alertar e abordar prontamente as falhas críticas de controle de segurança de acordo com todos os elementos especificados neste requisito. **A3.3.1.b** Examine os processos de detecção e alerta e entreviste a equipe para verificar se os processos estão implementados para todos os controles de segurança críticos especificados neste requisito e se cada falha de um controle de segurança crítico resulta na geração de um alerta.	**Objetivo** Sem processos formais para a detecção imediata (o mais rápido possível), alertas e endereçamento de falhas de controles de segurança críticos, as falhas podem não ser detectadas ou permanecer sem solução por longos períodos. Além disso, sem processos com limite de tempo formalizados, os atacantes terão tempo suficiente para comprometer os sistemas e roubar dados da conta do CDE. **Práticas Recomendadas** Os tipos específicos de falhas podem variar, dependendo da função do componente de sistema do dispositivo e da tecnologia em uso. Falhas típicas incluem um sistema que deixa de executar sua função de segurança ou não funciona da maneira pretendida, como um firewall apagando todas as suas regras ou ficando offline.

(continua na página a seguir)

Requisitos e Procedimentos de Teste		Diretriz
Objetivo da Abordagem Personalizada Este requisito não se aplica às abordagens personalizadas.		
Observações de Aplicabilidade *Os marcadores acima (para mecanismos automatizados de revisão de registro e ferramentas automatizadas de revisão de código (se usadas)) são as práticas recomendadas até 31 de março de 2025, após o qual serão exigidos como parte do Requisito A3.3.1 e devem ser totalmente considerados durante uma avaliação do PCI DSS.*		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** Se os alertas de falhas de sistemas de controle de segurança críticos não forem respondidos de forma rápida e eficaz, os invasores podem usar esse tempo para inserir software malicioso, obter o controle de um sistema ou roubar dados do ambiente da entidade. **Práticas Recomendadas** Evidências documentadas (por exemplo, registros em um sistema de gerenciamento de problemas) devem apoiar os processos e procedimentos implementados que respondem às falhas de segurança. Além disso, o pessoal deve estar ciente de suas responsabilidades em caso de falha. Ações e respostas à falha devem ser capturadas na evidência documentada.
A3.3.1.2 As falhas de qualquer sistema de controle de segurança crítico são respondidas prontamente. Os processos para responder a falhas nos sistemas de controle de segurança incluem: • Restaurar as 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, incluindo a causa raiz, e documentar a correção necessária para abordar a causa raiz. • 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. **Referência do PCI DSS**: *Requisitos 1 - 12*	**A3.3.1.2.a** Examinar as políticas e procedimentos documentados e entrevistar o pessoal para verificar se os processos são definidos e implementados para responder prontamente a uma falha de controle de segurança de acordo com todos os elementos especificados neste requisito	
	A3.3.1.2.b Examine os registros para verificar se as falhas de controle de segurança estão documentadas para incluir: • Identificação da(s) causa(s) da falha, incluindo a causa raiz. • Duração (data e hora de início ao fim) da falha de segurança. • Detalhes da correção necessária para resolver a causa raiz.	
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo** As tecnologias de hardware e software estão em constante evolução e as organizações precisam estar cientes das mudanças nas tecnologias que usam, bem como das ameaças em evolução a essas tecnologias. A realização de análises apropriadas dessas tecnologias garante que elas possam se preparar e gerenciar vulnerabilidades em hardware e software que não serão corrigidas pelo fornecedor ou desenvolvedor. **Práticas Recomendadas** As organizações também devem considerar a revisão das versões de firmware para garantir que permaneçam atuais e com suporte dos fornecedores. As organizações também precisam estar cientes das mudanças feitas pelos fornecedores de tecnologia em seus produtos ou processos para entender como tais mudanças podem impactar o uso da tecnologia pela organização. As análises regulares das tecnologias que impactam ou influenciam os controles do PCI DSS podem ajudar nas estratégias de compra, uso e implantação, e garantir que os controles que dependem dessas tecnologias permaneçam eficazes. Essas revisões incluem, mas não se limitam a, revisar tecnologias que não são mais suportadas pelo fornecedor e/ou não atendem mais às necessidades de segurança da organização.
A3.3.2 As tecnologias de hardware e software são revisadas pelo menos uma vez a cada 12 meses para confirmar se continuam atendendo aos requisitos do PCI DSS da organização. **Referência do PCI DSS**: *Requisitos 2, 6, 12.*	**A3.3.2.a** Examine as políticas e procedimentos documentados e entreviste o pessoal para verificar se os processos são definidos e implementados para revisar as tecnologias de hardware e software para confirmar se continuam atendendo aos requisitos do PCI DSS da organização.	
	A3.3.2.b Revise os resultados das revisões recentes de tecnologias de hardware e software para verificar se as revisões são realizadas pelo menos uma vez a cada 12 meses.	
Objetivo da Abordagem Personalizada Este requisito não se aplica às abordagens personalizadas.	**A3.3.2.c** Revise a documentação para verificar se, para quaisquer tecnologias que foram determinadas que não atendem mais aos requisitos do PCI DSS da organização, existe um plano para remediar a tecnologia.	
Observações de Aplicabilidade O processo inclui um plano para remediação de tecnologias que não atendem mais aos requisitos do PCI DSS da organização, até e incluindo a substituição da tecnologia, conforme apropriado.		

Requisitos e Procedimentos de Teste		Diretriz
Requisitos da Abordagem Definida	**Procedimentos de Teste da Abordagem Definida**	**Objetivo**
A3.3.3 As revisões são realizadas pelo menos uma vez a cada três meses para verificar se as atividades BAU estão sendo seguidas. As revisões são realizadas por pessoal designado ao programa de conformidade com o PCI DSS (conforme identificado em A3.1.3) e incluem: • Confirmação de que todas as atividades BAU, incluindo A3.2.2, A3.2.6 e A3.3.1, estão sendo realizadas. • Confirmação de que o pessoal está seguindo as políticas de segurança e procedimentos operacionais (por exemplo, revisões diárias de registro, revisões de conjunto de regras para controles de segurança de rede, padrões de configuração para novos sistemas) • Documentar como as revisões foram concluídas, incluindo como todas as atividades BAU foram verificadas como estando implementadas. • Coleta de evidências documentadas conforme necessário para a avaliação anual do PCI DSS. • Revisão e aprovação dos resultados pela equipe com responsabilidade pelo programa de conformidade com o PCI DSS, conforme identificado em A3.1.3. • Retenção de registros e documentação por pelo menos 12 meses, cobrindo todas as atividades BAU. **Referência do PCI DSS**: *Requisitos 1 - 12*	**A3.3.3.a** Examine as políticas e procedimentos para verificar se os processos estão definidos para revisar e verificar as atividades BAU de acordo com todos os elementos especificados neste requisito. **A3.3.3.b** Entreviste o pessoal responsável e examine os registros das revisões para verificar se: • As revisões são realizadas por pessoal designado ao programa de conformidade com o PCI DSS. • As revisões são realizadas pelo menos uma vez a cada três meses.	A confirmação regular de que as políticas e procedimentos de segurança estão sendo seguidos fornece a garantia de que os controles esperados estão ativos e funcionando conforme pretendido. O objetivo dessas revisões não é realizar novamente outros requisitos do PCI DSS, mas confirmar se as atividades de segurança estão sendo executadas continuamente. **Práticas Recomendadas** Essas revisões também podem ser usadas para verificar se a evidência apropriada está sendo mantida - por exemplo, registros de auditoria, relatórios de varredura de vulnerabilidade, revisões de conjuntos de regras de controle de segurança de rede - para auxiliar na preparação da entidade para sua próxima avaliação do PCI DSS. **Exemplos** Tomando o Requisito 1.2.7 como um exemplo, o Requisito A3.3.3 é atendido pela confirmação, pelo menos uma vez a cada três meses, de que as revisões das configurações dos controles de segurança da rede ocorreram na frequência necessária. Por outro lado, o Requisito 1.2.7 é atendido pela revisão das configurações conforme especificado no requisito.
Objetivo da Abordagem Personalizada		
Este requisito não se aplica às abordagens personalizadas.		

Requisitos e Procedimentos de Teste		Diretriz
A3.4 O acesso lógico ao ambiente de dados do titular do cartão é controlado e gerenciado.		
Requisitos da Abordagem Definida **A3.4.1** As contas do usuário e os privilégios de acesso aos componentes de sistema no escopo são revisados pelo menos uma vez a cada seis meses para garantir que as contas do usuário e os privilégios de acesso permaneçam apropriados com base na função do trabalho e que todo o acesso seja autorizado. **Referência do PCI DSS**: *Requisito 7* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.	**Procedimentos de Teste da Abordagem Definida** **A3.4.1** Entreviste o pessoal responsável e examine a documentação de apoio para verificar se: • As contas de usuário e os privilégios de acesso são revisados pelo menos a cada seis meses. • As revisões confirmam que o acesso é apropriado com base na função de trabalho e que todo o acesso está autorizado.	**Objetivo** A revisão regular dos direitos de acesso ajuda a detectar direitos de acesso excessivos remanescentes depois que as responsabilidades do trabalho do usuário mudam, as funções do sistema mudam ou outras modificações. Se direitos excessivos do usuário não forem revogados no devido tempo, eles podem ser usados por usuários mal-intencionados para acesso não autorizado. Essa revisão fornece outra oportunidade para garantir que as contas de todos os usuários desligados tenham sido removidas (se alguma delas tiver sido perdida no momento do desligamento), bem como para garantir que quaisquer terceiros que não precisam mais de acesso tenham seu acesso encerrado.

Requisitos e Procedimentos de Teste		Diretriz
A3.5 Eventos suspeitos são identificados e respondidos.		
Requisitos da Abordagem Definida **A3.5.1** Uma metodologia é implementada para a identificação imediata de padrões de ataque e comportamento indesejável em sistemas que inclui: • Identificação de anomalias ou atividades suspeitas à medida que ocorrem. • Emissão de alertas imediatos ao detectar atividades suspeitas ou anomalias ao pessoal responsável. • Resposta a alertas de acordo com procedimentos de resposta documentados. **Referência do PCI DSS**: *Requisitos 10, 12* **Objetivo da Abordagem Personalizada** Este requisito não se aplica às abordagens personalizadas.	**Procedimentos de Teste da Abordagem Definida** **A3.5.1.a** Examine a documentação e entreviste o pessoal para verificar se uma metodologia foi definida e implementada para identificar padrões de ataque e comportamento indesejável nos sistemas de maneira imediata e inclui todos os elementos especificados neste requisito. **A3.5.1.b** Examine os procedimentos de resposta a incidentes e entreviste o pessoal responsável para verificar se: • O pessoal de plantão recebe alertas imediatos. • Os alertas são respondidos de acordo com os procedimentos de resposta documentados.	**Objetivo** A capacidade de identificar padrões de ataque e comportamento indesejável em sistemas - por exemplo, usando ferramentas de correlação de registro gerenciadas centralmente ou automatizadas - é crítica para prevenir, detectar ou minimizar o impacto de um comprometimento de dados. A presença de registros em todos os ambientes permite rastreamento, alerta e análise completos quando algo dá errado. Determinar a causa de um comprometimento é muito difícil, senão impossível, sem um processo para corroborar informações de componentes críticos de sistema e sistemas que executam funções de segurança, como controles de segurança de rede, IDS/IPS e sistemas de monitoramento de integridade de arquivos (FIM). Portanto, os registros de todos os componentes de sistema críticos e sistemas que executam funções de segurança precisam ser coletados, correlacionados e mantidos. Isso pode incluir o uso de produtos de software e metodologias de serviço para fornecer análises, alertas e relatórios em tempo real, como sistemas de gerenciamento de eventos e informações de segurança (SIEM), FIM ou detecção de alterações.

Apêndice B Controles de Compensação

Os controles de compensação podem ser considerados quando uma entidade não pode atender a um requisito do PCI DSS explicitamente conforme declarado, devido a restrições técnicas ou comerciais legítimas e documentadas, mas mitigou suficientemente o risco associado ao requisito por meio da implementação de outros controles de compensação.

Os controles de compensação devem satisfazer os seguintes critérios:

1. Atender à intenção e ao rigor do requisito original do PCI DSS.
2. Fornecer um nível de defesa semelhante ao do requisito original do PCI DSS, de modo que o controle de compensação compensa suficientemente o risco contra o qual o requisito original do PCI DSS foi projetado para se defender. Para entender a intenção de um requisito, consulte *o Objetivo da Abordagem Personalizada* para a maioria dos requisitos do PCI DSS. Se um requisito não for elegível para a abordagem personalizada e, portanto, não tiver um *Objetivo da Abordagem Personalizada*, consulte o **Objetivo** na coluna Diretriz para esse requisito.
3. Estar “acima e além” de outros requisitos do PCI DSS. (Simplesmente estar em conformidade com outros requisitos do PCI DSS não é um controle de compensação.)
4. Ao avaliar "acima e além" para controles de compensação, considere o seguinte:

Observação: *Todos os controles de compensação devem ser revisados e validados quanto à suficiência pelo assessor que conduz a avaliação do PCI DSS. A eficácia de um controle de compensação depende das especificações do ambiente no qual o controle é implementado, dos controles de segurança circundantes e da configuração do controle. As entidades devem estar cientes de que um determinado controle de compensação não será eficaz em todos os ambientes.*

a. Os requisitos existentes do PCI DSS NÃO PODEM ser considerados como controles de compensação se já forem exigidos para o item em análise. Por exemplo, as senhas para acesso administrativo não-console devem ser enviadas criptografadas para mitigar o risco de interceptar senhas administrativas em texto não criptografado. Uma entidade não pode usar outros requisitos de senha do PCI DSS (bloqueio de intrusão, senhas complexas, etc.) para compensar a falta de senhas criptografadas, uma vez que esses outros requisitos de senha não reduzem o risco de interceptação de senhas em texto não criptografado. Além disso, os outros controles de senha já são requisitos do PCI DSS para o item em revisão (senhas).
b. Os requisitos existentes do PCI DSS PODEM ser considerados como controles de compensação se forem necessários para outra área, mas não para o item em análise.

c. Os requisitos existentes do PCI DSS podem ser combinados com novos controles para se tornarem um controle de compensação. Por exemplo, se uma empresa não consegue resolver uma vulnerabilidade que pode ser explorada por meio de uma interface de rede porque uma atualização de segurança ainda não está disponível por um fornecedor, um controle de compensação pode consistir em controles que incluem todos os seguintes: 1) segmentação de rede interna, 2) limitar o acesso pela rede à interface vulnerável apenas aos dispositivos necessários (filtragem de endereço IP ou endereço MAC) e 3) monitoramento com IDS/IPS de todo o tráfego destinado à interface vulnerável.

5. Abordar o risco adicional imposto por não cumprir os requisitos do PCI DSS.

6. Atender aos requisitos atuais e futuros. Um controle de compensação não pode atender a um requisito que foi perdido no passado (por exemplo, onde a execução de uma tarefa foi exigida há dois trimestres, mas essa tarefa não foi executada).

O assessor deve avaliar exaustivamente os controles de compensação durante cada avaliação anual do PCI DSS para confirmar se cada controle de compensação trata de forma adequada o risco que o requisito original do PCI DSS foi projetado para abordar, de acordo com os itens 1-6 acima.

Para manter a conformidade, os processos e controles devem estar implementados para garantir que os controles de compensação permaneçam eficazes após a conclusão da avaliação. Além disso, os resultados do controle de compensação devem ser documentados no relatório aplicável para a avaliação (por exemplo, um relatório sobre conformidade ou um questionário de autoavaliação) na seção de requisitos do PCI DSS correspondente e incluídos quando o relatório aplicável for enviado à organização solicitante .

Apêndice C Planilha de Controles de Compensação

A entidade deve usar esta planilha para definir os controles de compensação para qualquer requisito onde os controles de compensação são usados para atender a um requisito do PCI DSS. Observe que os controles de compensação também devem ser documentados de acordo com as instruções no relatório sobre conformidade na seção de requisitos do PCI DSS correspondente.

Observação: *Somente as entidades que possuem restrições tecnológicas ou comerciais legítimas e documentadas podem considerar o uso de controles de compensação para atingir a conformidade.*

Número e Definição do Requisito:

	Informações Requeridas	Explicação
1. Restrições	Documente as restrições técnicas ou comerciais legítimas que impedem a conformidade com o requisito original.	
2. Definição dos Controles de Compensação	Defina os controles de compensação: explique como eles abordam os objetivos do controle original e o risco aumentado, se houver.	
3. Objetivo	Defina o objetivo do controle original (por exemplo, o Objetivo da Abordagem Personalizada).	
	Identifique o objetivo atendido pelo controle de compensação (*observação: pode ser, mas não é obrigatório, o Objetivo de Abordagem Personalizada declarado para o requisito do 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 D Abordagem Personalizada

Esta abordagem é destinada a entidades que decidem atender a um Objetivo da Abordagem Personalizada declarado em um requisito do PCI DSS de uma forma que não segue estritamente o requisito definido. A abordagem personalizada permite que uma entidade adote uma abordagem estratégica para atender ao Objetivo da Abordagem Personalizada de um requisito, para que possa determinar e projetar os controles de segurança necessários para atender ao objetivo de uma maneira única para essa organização.

A entidade que implementa uma abordagem personalizada deve atender aos seguintes critérios:

- Documentar e manter evidências sobre cada controle personalizado, incluindo todas as informações especificadas no Modelo de Matriz de Controles no Apêndice E1.
- Realizar e documentar uma análise de risco direcionada (Requisito 12.3.2 do PCI DSS) para cada controle personalizado, incluindo todas as informações especificadas no Modelo de Análise de Risco Direcionada no Apêndice E2.
- Realizar o teste de cada controle personalizado para provar a eficácia e documentar os testes realizados, os métodos usados, o que foi testado, quando o teste foi realizado e os resultados dos testes na matriz de controles.
- Monitorar e manter evidências sobre a eficácia de cada controle personalizado.
- Fornecer matriz(es) de controle preenchida(s), análise de risco direcionada, evidência de teste e evidência de eficácia do controle personalizado para seu assessor.

O assessor que realiza uma avaliação dos controles personalizados deve atender aos seguintes critérios:

- Revisar a(s) matriz(s) de controles da entidade, a análise de risco direcionada e a evidência da eficácia do controle para compreender totalmente o(s) controle(s) personalizado(s) e verificar se a entidade atende a todos os requisitos de documentação e evidência da Abordagem Personalizada.
- Derivar e documentar os procedimentos de teste apropriados necessários para conduzir o teste completo de cada controle personalizado.
- Testar cada controle personalizado para determinar se a implementação da entidade 1) atende ao objetivo da abordagem personalizada do requisito e 2) resulta em uma conclusão de "implementado" para o requisito.
- Em todos os momentos, os QSAs mantêm os requisitos de independência definidos nos Requisitos de Qualificação do QSA. Isso significa que se um QSA estiver envolvido no projeto ou implementação de um controle personalizado, esse QSA não derivará também procedimentos de teste para avaliar ou auxiliar na avaliação desse controle personalizado.

Espera-se que a entidade e seu assessor trabalhem juntos para garantir que 1) concordam que o(s) controle(s) personalizado(s) atende(m) totalmente ao objetivo da abordagem personalizada, 2) o assessor entende totalmente o controle personalizado e 3) a entidade entende o teste derivado que o assessor irá realizar.

O uso da abordagem personalizada deve ser concluído por um QSA ou ISA e documentado de acordo com as instruções no modelo de Relatório sobre Conformidade (ROC) e seguindo as instruções nas *FAQs para uso com o modelo de ROC do PCI DSS v4.0 disponível no website do PCI SSC*.

As entidades que completam um Questionário de Autoavaliação não são elegíveis para usar uma abordagem personalizada; no entanto, essas entidades podem decidir que um QSA ou ISA execute sua avaliação e a documente em um modelo de ROC.

O uso da abordagem personalizada pode ser regulamentado por organizações que gerenciam programas de conformidade (por exemplo, bandeiras de pagamento e adquirentes). Portanto, perguntas sobre o uso de uma abordagem personalizada devem ser encaminhadas a essas organizações, incluindo, por exemplo, se uma entidade é obrigada a usar um QSA ou pode usar um ISA para concluir uma avaliação usando a abordagem personalizada.

Observação: *Os controles de compensação não são uma opção com a abordagem personalizada. Como a abordagem personalizada permite que uma entidade determine e projete os controles necessários para atender ao Objetivo da Abordagem Personalizada de um requisito, espera-se que a entidade implemente de forma eficaz os controles projetados para esse requisito, sem a necessidade de também implementar controles alternativos de compensação.*

Apêndice E Amostra de Modelos para Apoiar a Abordagem Personalizada

Este apêndice contém exemplo de modelos para a matriz de controles e uma análise de risco direcionada, a ser documentada pela entidade como parte da abordagem personalizada. Esses modelos são exemplos de formatos que podem ser usados. *Embora não seja necessário que as entidades sigam os formatos específicos fornecidos neste apêndice, a matriz de controle da entidade e a análise de risco direcionada devem incluir todas as informações definidas nesses modelos.*

E1 Amostra de Modelo de Matriz de Controles

A seguir está uma amostra de modelo de matriz de controles que uma entidade pode usar para documentar sua implementação personalizada.

Conforme descrito no *Apêndice D*: *Abordagem Personalizada,* as entidades que usam a abordagem personalizada devem preencher uma matriz de controles para fornecer detalhes para cada controle implementado que explica o que é implementado, como a entidade determinou que os controles atendem ao objetivo declarado de um requisito do PCI DSS, como o controle fornece pelo menos o nível equivalente de proteção que seria alcançado pelo cumprimento do requisito definido, e como a entidade tem garantia sobre a eficácia do controle em uma base contínua.

O assessor usa as informações de cada matriz de controle para planejar e se preparar para a avaliação.

Esta amostra de modelo de matriz de controle inclui as informações mínimas a serem documentadas pela entidade e fornecidas ao assessor para uma validação personalizada. Embora não seja necessário que este modelo específico seja usado, é necessário que a documentação da abordagem personalizada da entidade inclua todas as informações definidas neste modelo e que a entidade forneça essas informações exatas ao seu assessor.

A matriz de controles não substitui a necessidade do assessor desenvolver de forma independente procedimentos de teste apropriados para validar os controles implementados. O assessor deve ainda realizar os testes necessários para verificar se os controles atendem ao objetivo do requisito, são eficazes e estão devidamente mantidos. A matriz de controles também não substitui os requisitos de relatório para validações personalizadas conforme especificado no Modelo de ROC.

A matriz de controles deve incluir pelo menos as informações da tabela a seguir.

Amostra de Modelo de Matriz de Controle para Requisitos do PCI DSS atendidos por meio da Abordagem Personalizada A ser preenchido pela entidade que está sendo avaliada		
Nome/identificador de controle personalizado	<A entidade define como eles querem se referir a este controle>	
Número(s) e objetivo(s) do(s) requisito(s) do PCI DSS atendidos com este(s) controle(s)	Requisito No.: Requisito No.:	Objetivo: Objetivo:
Detalhes do(s) controle(s)		
Qual é o controle(s) implementado?	<A entidade descreve o que é o controle e o que ele faz>	
Onde o(s) controle(s) são implementados?	<A entidade identifica os locais das instalações e componentes de sistema onde o controle é implementado e gerenciado>	
Quando o(s) controle(s) são realizados?	<A entidade detalha com que frequência o controle é realizado - por exemplo, é executado continuamente em tempo real ou está programado para ser executado em NN vezes e em intervalos XX>	
Quem tem responsabilidade geral e responsabilização pelo(s) controle(s)?	<A entidade inclui detalhes de funcionários/funções individuais com responsabilidade e responsabilização por este controle>	
Quem está envolvido no gerenciamento, manutenção e monitoramento do(s) controle(s)?	<A entidade inclui detalhes de pessoal/funções e/ou equipes individuais, conforme aplicável, que gerenciam, mantêm e monitoram o controle>	
***Para cada* requisito do PCI DSS para o qual o(s) controle(s) são usados, a entidade fornece detalhes do seguinte:**		
A entidade descreve como o(s) controle(s) implementado(s) atendem ao ***Objetivo da Abordagem Personalizada*** declarado no requisito do PCI DSS.	<A entidade descreve como o controle atende ao objetivo de abordagem personalizada declarado no requisito do PCI DSS e resume os resultados relacionados>	

Amostra de Modelo de Matriz de Controle para Requisitos do PCI DSS atendidos por meio da Abordagem Personalizada A ser preenchido pela entidade que está sendo avaliada	
A entidade descreve os testes **realizados** e os resultados desses testes que demonstram que o(s) controle(s) atendem ao objetivo do requisito aplicável.	<A entidade descreve o teste realizado para provar que o controle atende ao objetivo declarado no requisito do PCI DSS e resume os resultados relacionados>
A entidade descreve resumidamente os resultados da análise de risco direcionada **realizada** separadamente que explica o(s) controle(s) implementado(s) e descreve como os resultados verificam se o(s) controle(s) fornecem pelo menos um nível equivalente de proteção como a abordagem definida para o requisito do PCI DSS aplicável . *Consulte o Modelo de Análise de Risco Direcionada para obter detalhes sobre como documentar essa análise de risco.*	<A entidade descreve resumidamente os resultados de sua análise de risco para este controle, que é detalhada separadamente na Análise de Risco Direcionada>
A entidade descreve as medidas que **implementou** para garantir que o(s) controlo(s) seja(am) mantido(s) e a sua eficácia assegurada de forma contínua. *Por exemplo, como a entidade monitora a eficácia do controle, como as falhas do controle são detectadas e respondidas, e as ações tomadas.*	<A entidade descreve como ela garante que o controle seja mantido e como a eficácia do controle é garantida.>

E2 Amostra de Modelo de Análise de Risco Direcionada

A seguir está uma amostra de modelo de análise de risco direcionada que uma entidade pode usar para sua implementação personalizada. *Embora não seja necessário que uma entidade siga este formato específico, sua documentação de abordagem personalizada deve incluir todas as informações definidas neste modelo.*

Conforme descrito no *Apêndice D*: *Abordagem Personalizada* e de acordo com o Requisito 12.3.2 do PCI DSS, uma entidade que usa a abordagem personalizada deve fornecer uma análise de risco direcionada detalhada para cada requisito que a entidade está atendendo com a abordagem personalizada. A análise de risco define o risco, avalia o efeito na segurança se o requisito definido não for atendido e descreve como a entidade determinou que os controles fornecem pelo menos um nível equivalente de proteção conforme fornecido pelo requisito do PCI DSS definido.

O assessor usa as informações na análise de risco direcionada para planejar e se preparar para a avaliação.

Ao concluir uma análise de risco direcionada para uma abordagem personalizada, é importante lembrar que:

- O ativo que está sendo protegido são os dados do titular do cartão que são armazenados, processados ou transmitidos pela entidade.
- O ator da ameaça é altamente motivado e capaz. A motivação e a capacidade dos agentes de ameaças tendem a aumentar em relação ao volume de dados do titular do cartão para a realização de um ataque bem-sucedido.
- A probabilidade de uma entidade ser alvo de ameaças aumenta à medida que a entidade armazena, processa ou transmite maiores volumes de dados do titular do cartão.
- O dano está diretamente relacionado ao objetivo. Por exemplo, se o objetivo for “o software malicioso não pode ser executado”, o dano é que o software malicioso é executado; se o objetivo é “responsabilidades do dia-a-dia para a execução de todas as atividades são alocadas”, o dano é que as responsabilidades não são alocadas.

Observação: *O termo “dano” conforme usado nesta análise de risco direcionada (por exemplo, no 1.3 da tabela abaixo) se refere a uma ocorrência ou evento que afeta negativamente a postura de segurança da entidade. Exemplos disso são a ausência de uma política, a falha em conduzir uma verificação de vulnerabilidade ou que malware é executado no ambiente da entidade.*

Esta amostra de modelo de análise de risco direcionada inclui as informações mínimas a serem documentadas pela entidade e fornecidas ao assessor para uma validação personalizada. Embora não seja necessário que este modelo específico seja usado, é necessário que a documentação de abordagem personalizada da entidade inclua todas as informações definidas neste modelo e que a entidade forneça essas informações exatas ao seu assessor.

A análise de risco direcionada deve incluir pelo menos as informações da tabela a seguir.

Amostra de análise de risco direcionada para requisitos do PCI DSS atendidos por meio da Abordagem Personalizada A ser preenchido pela entidade que está sendo avaliada	
Item	**Detalhes**
1. Identificar o requisito	
1.1 Identifique o requisito do PCI DSS conforme escrito.	<A entidade identifica o requisito>
1.2 Identifique o objetivo do requisito do PCI DSS conforme escrito.	<A entidade identifica o objetivo do requisito>
1.3 Descreva o dano que o requisito foi projetado para prevenir	<A entidade descreve o dano> <A entidade descreve o efeito em sua segurança se o objetivo não for alcançado com sucesso pela entidade.> <A entidade descreve quais fundamentos de segurança não estariam implementados, ou o que um agente de ameaça pode ser capaz de fazer se o objetivo não for alcançado com sucesso pela entidade.>
2. Descrever a solução proposta	
2.1 Nome/identificador de controle personalizado	<A entidade identifica o controle personalizado conforme documentado na Matriz de Controles.>
2.2 Quais partes do requisito conforme escrito serão alteradas na solução proposta?	<A entidade identifica quais elementos do requisito não serão atendidos pela abordagem definida e, portanto, serão cobertos pela abordagem personalizada. Isso pode ser tão pequeno quanto alterar a periodicidade de um requisito ou a implementação de um conjunto de controles completamente diferente para atender ao objetivo.>
2.3 Como a solução proposta evitará o dano?	<A entidade descreve como os controles detalhados na Matriz de Controles evitarão o dano identificado em 1.3.>

Amostra de análise de risco direcionada para requisitos do PCI DSS atendidos por meio da Abordagem Personalizada A ser preenchido pela entidade que está sendo avaliada						
Item	**Detalhes**					
3. Examine todas as alterações na PROBABILIDADE de ocorrência do dano, levando a uma violação da confidencialidade dos dados do titular do cartão						
3.1 Descreva os fatores detalhados na Matriz de Controle que afetam a probabilidade de ocorrência do dano.	A entidade descreve: • O quanto os controles serão bem sucedidos na prevenção dos danos • Como os controles detalhados na Matriz de Controle reduzem a probabilidade de ocorrência dos danos					
3.2 Descreva as razões pelas quais o dano ainda pode ocorrer após a aplicação do controle personalizado.	A entidade descreve: • Os motivos típicos para a falha do controle, a probabilidade disso e como isso poderia ser evitado • Quão resilientes os processos e sistemas da entidade são para detectar que o(s) controle(s) não estão operando normalmente? • Como um agente da ameaça poderia ignorar esse controle - quais etapas eles precisariam seguir, quão difícil é, o agente da ameaça seria detectado antes que o controle falhasse? Como isso foi determinado?					
3.3 Até que ponto os controles detalhados na abordagem personalizada representam uma mudança na probabilidade de ocorrência do dano em comparação com o requisito da abordagem definida?	Dano com mais probabilidade de acontecer	☐	Sem mudanças	☐	Dano com menos probabilidade de acontecer	☐
3.4 Forneça o raciocínio para sua avaliação da mudança na probabilidade do dano ocorrer depois que os controles personalizados estiverem implementados.	A entidade oferece: • A justificativa para a avaliação documentada em 3.3. • Os critérios e valores usados para a avaliação documentada em 3.3.					

Amostra de análise de risco direcionada para requisitos do PCI DSS atendidos por meio da Abordagem Personalizada A ser preenchido pela entidade que está sendo avaliada				
Item	**Detalhes**			
4. Examine todas as alterações no IMPACTO do acesso não autorizado aos dados da conta				
4.1 Para o escopo dos componentes de sistema que esta solução cobre, qual volume de dados da conta estaria em risco de acesso não autorizado se a solução falhasse?	**4.1.1** Número de PANs armazenados	*Máximo a qualquer momento*	**4.1.2** Número de PANs processados ou transmitidos em um período de 12 meses	*Total*
4.2 Descrição de como os controles personalizados irão diretamente: • Reduzir o número de PANs individuais comprometidos se um ator de ameaça for bem-sucedido e/ou • Permitir notificação mais rápida dos PANs comprometidos com as bandeiras de cartões.	O impacto no ecossistema de pagamento está diretamente relacionado ao número de contas comprometidas e a rapidez com que quaisquer PANs comprometidos podem ser bloqueados pelo emissor do cartão Entidade descreve como os controles personalizados alcançam o seguinte se algum dos controles personalizados: • Reduzir o volume de dados do titular do cartão que são armazenados, processados ou transmitidos e, portanto, reduzir o que está disponível para um ator de ameaça bem-sucedido e/ou • Diminua o tempo de detecção, notificação de contas comprometidas e contenção do ator da ameaça.			
5. Aprovação e revisão do risco				
5.1 Eu revisei a análise de risco acima e concordo que o uso da abordagem personalizada proposta conforme detalhado fornece pelo menos um nível equivalente de proteção como a abordagem definida para o requisito aplicável do PCI DSS.	Um membro da gestão executiva deve revisar e concordar com a abordagem personalizada proposta. <O membro da gestão executiva da entidade assina que analisou e concordou com a abordagem personalizada aqui documentada.>			
5.2 Esta análise de risco deve ser revisada e atualizada o mais tardar:	A análise de risco deve ser revisada pelo menos a cada doze meses e com mais frequência se a abordagem personalizada em si for limitada no tempo (por exemplo, porque há uma mudança planejada na tecnologia) ou se outros fatores ditarem uma mudança necessária. No caso de uma revisão de risco não programada, detalhe o motivo da revisão. <A entidade indica a data em que a análise de risco alvo foi revisada e atualizada.>			

Apêndice F Aproveitando a Estrutura de Segurança de Software do PCI para Atender ao Requisito 6

O Requisito 6 do PCI DSS define os requisitos para o desenvolvimento e manutenção de sistemas e software seguros. Como o Padrão de Software Seguro e o Padrão de SLC Seguro do PCI SSC (coletivamente, a Estrutura de Segurança do Software) incluem requisitos de segurança de software rigorosos, o uso de software sob medida e personalizado desenvolvido e mantido de acordo com qualquer um dos padrões pode ajudar a entidade a atender a vários requisitos no Requisito 6 do PCI DSS sem a necessidade de realizar testes detalhados adicionais e também pode oferecer suporte ao uso da Abordagem Personalizada para outros requisitos. Para mais detalhes, consulte a Tabela 7.

***Observação**: Este suporte para cumprir o Requisito 6 aplica-se apenas ao software especificamente desenvolvido e mantido de acordo com o Padrão de Software Seguro ou o Padrão de SLC Seguro; não se estende a outro software ou componentes de sistema no escopo do Requisito 6.*

Tabela 7. Aproveitando a Estrutura de Segurança de Software do PCI para Atender ao Requisito 6

Requisitos do PCI DSS	Como os Requisitos do PCI DSS se Aplicam ao Software Desenvolvido e Mantido de Acordo com o Padrão de Software Seguro	Como os Requisitos do PCI DSS se Aplicam ao Software Desenvolvido e Mantido de Acordo com o Padrão de SLC Seguro
6.1 Os processos e mecanismos para executar as atividades no Requisito 6 são definidos e compreendidos.	Os requisitos/objetivos do PCI DSS se aplicam normalmente.	
6.2 O software sob medida e personalizado é desenvolvido com segurança.	O Requisito 6.2.4 do PCI DSS pode ser considerado implementado para software desenvolvido e mantido de acordo com o Padrão de Software Seguro.	O Requisito 6.2 do PCI DSS pode ser considerado implementado para software desenvolvido e mantido de acordo com o Padrão de SLC Seguro.
6.3 As vulnerabilidades de segurança são identificadas e prontamente resolvidas.	Os requisitos/objetivos do PCI DSS se aplicam normalmente. O software desenvolvido e mantido de acordo com o Padrão de SLC Seguro pode suportar a abordagem personalizada para os objetivos do Requisito 6.3. Embora o uso de software desenvolvido e mantido de acordo com o Padrão de SLC Seguro forneça garantia de que o fornecedor disponibiliza patches de segurança e atualizações de software em tempo hábil, **a entidade mantém a responsabilidade** de garantir que os patches e atualizações sejam instalados de acordo com os requisitos do PCI DSS.	

Requisitos do PCI DSS	Como os Requisitos do PCI DSS se Aplicam ao Software Desenvolvido e Mantido de Acordo com o Padrão de Software Seguro	Como os Requisitos do PCI DSS se Aplicam ao Software Desenvolvido e Mantido de Acordo com o Padrão de SLC Seguro
6.4 Os aplicativos web voltados para o público são protegidos contra ataques.	Os requisitos/objetivos do PCI DSS se aplicam normalmente.	
6.5 As mudanças em todos os componentes de sistema são gerenciadas com segurança.	Os requisitos/objetivos do PCI DSS se aplicam normalmente. O software desenvolvido e mantido de acordo com o Padrão de SLC Seguro pode suportar a abordagem personalizada para os objetivos do Requisito 6.5. Embora o uso de software desenvolvido e mantido de acordo com o Padrão SLC Seguro forneça garantia de que o fornecedor segue os procedimentos de gerenciamento de mudanças durante o desenvolvimento de software e atualizações relacionadas, **a entidade mantém a responsabilidade** de garantir que o software e outras mudanças nos componentes de sistema sejam implementados em seu ambiente de produção acordo com os requisitos do PCI DSS.	

Uso de software sob medida e personalizado desenvolvido e mantido por um Fornecedor Qualificado de SLC Seguro

Ao validar o uso de software desenvolvido e mantido por um Fornecedor Qualificado de SLC seguro para atender ao Requisito 6.2 do PCI DSS e apoiar a Abordagem Personalizada para os Requisitos 6.3 e 6.5, o assessor deve confirmar se o seguinte é atendido:

- O fornecedor do software está atualmente listado na lista do PCI SSC de Fornecedores Qualificados de SLC Seguro - ou seja, a validação não expirou.
- O software foi desenvolvido e está sendo mantido usando práticas de gerenciamento de ciclo de vida de software que foram avaliadas como parte da validação do fornecedor de software.
- A entidade está seguindo a orientação de implementação fornecida pelo Fornecedor Qualificado de SLC Seguro.

Uso de software sob medida e personalizado desenvolvido de acordo com o Padrão de SLC Seguro

As entidades que desenvolvem software internamente exclusivamente para seu uso ou que desenvolvem software para uso por uma única entidade podem optar por contratar um Assessor de SLC Seguro para avaliar suas práticas de gerenciamento de ciclo de vida de software em relação ao Padrão de SLC Seguro. O Assessor de SLC Seguro documentará os resultados da avaliação em um Relatório sobre Conformidade de SLC Seguro (ROC) e um Atestado de Conformidade de SLC Seguro (AOC).

O software que é desenvolvido e mantido de acordo com as práticas de gerenciamento do ciclo de vida do software fornece o mesmo suporte para o Requisito 6 do PCI DSS que o software desenvolvido e mantido por um Fornecedor Qualificado de SLC Seguro, se essas práticas foram avaliadas por um Assessor de SLC Seguro e confirmadas para atender aos requisitos do Padrão de SLC Seguro, com os resultados documentados em um ROC e AOC de SLC Seguro.

Validando o Uso do Padrão de SLC Seguro

Ao validar o uso de software desenvolvido e mantido de acordo com o Padrão de SLC Seguro para atender ao Requisito 6.2 do PCI DSS e apoiar a abordagem personalizada para os Requisitos 6.3 e 6.5, o assessor deve confirmar se o seguinte foi atendido:

- As práticas de gerenciamento do ciclo de vida do software foram avaliadas por um Assessor de SLC Seguro e confirmado para atender a todos os requisitos do Padrão de SLC Seguro com os resultados documentados em um Relatório sobre Conformidade de SLC Seguro (ROC) e Atestado de Conformidade de SLC Seguro (AOC).
- O software foi desenvolvido e mantido usando as práticas de gerenciamento do ciclo de vida do software cobertas pela avaliação de SLC Seguro.
- Uma avaliação completa de SLC Seguro das práticas de gerenciamento do ciclo de vida do software foi concluída nos 36 meses anteriores. Além disso, se a avaliação de SLC Seguro completa mais recente ocorreu há mais de 12 meses, um atestado anual foi fornecido pelo desenvolvedor/fornecedor nos 12 meses anteriores que confirma a adesão contínua ao Padrão de SLC Seguro para as práticas de gerenciamento do ciclo de vida do software em uso.

Validando o Uso do Padrão de Software Seguro

Ao validar o uso de software desenvolvido e mantido de acordo com o Padrão de Software Seguro para atender ao Requisito 6.2.4 do PCI DSS e apoiar a abordagem personalizada para os Requisitos 6.3 e 6.5, o assessor deve confirmar se o seguinte foi atendido:

- A avaliação de software seguro foi conduzida por um Assessor de Software Seguro e confirmada para atender a todos os requisitos no Padrão de Software Seguro com os resultados documentados em um Relatório de Validação de Software Seguro (ROV) e Atestado de Validação de Software Seguro (AOV).
- O software foi desenvolvido e está sendo mantido usando as práticas de gerenciamento do ciclo de vida do software que foram cobertas pela avaliação de software seguro.
- Uma avaliação completa de software seguro foi concluída nos 36 meses anteriores. Além disso, se a avaliação completa de software seguro mais recente ocorreu há mais de 12 meses, um atestado anual foi fornecido pelo desenvolvedor/fornecedor nos 12 meses anteriores que confirma a adesão contínua ao Padrão de Software Seguro.

Apêndice G Glossário de Termos, Abreviações e Acrônimos do PCI DSS

Termo	Definição
Abordagem Definida	Consulte a "*Seção 8 do PCI DSS: Abordagens para Implementação e Validação do PCI DSS"*
Abordagem Personalizada	Consulte a "*Seção 8 do PCI DSS: Abordagens para Implementação e Validação do PCI DSS"*
Acesso Administrativo	Privilégios elevados ou aumentados concedidos a uma conta para essa conta gerenciar sistemas, redes e/ou aplicativos. O acesso administrativo pode ser atribuído à conta de um indivíduo ou a uma conta de sistema integrada. As contas com acesso administrativo são frequentemente chamadas de "superusuário", "root", "administrador", "admin", "sysadmin" ou "estado de supervisor", dependendo do sistema operacional e da estrutura organizacional em particular.
Acesso não-console	Acesso lógico a um componente de sistema que ocorre por meio de uma interface de rede em vez de uma conexão física direta ao componente de sistema. O acesso não-console inclui acesso por redes locais/internas, bem como acesso por redes externas ou remotas.
Acesso Remoto	Acesso à rede de uma entidade de um local fora dessa rede. Um exemplo de tecnologia para acesso remoto é uma VPN.
Adquirente	Também conhecido como "banco do comerciante", "banco adquirente" ou "instituição financeira adquirente". Entidade, normalmente uma instituição financeira, que processa transações de cartão de pagamento para comerciantes e é definida por uma bandeira de pagamento como adquirente. Os adquirentes estão sujeitos às regras e procedimentos da bandeira de pagamento em relação à conformidade do comerciante. Consulte o *Processador de Pagamento*.
AES	Acrônimo para "Advanced Encryption Standard [Padrão de Criptografia Avançada]". Consulte *Criptografia Forte.*
Algoritmo de Criptografia	Também conhecido como "algoritmo de encriptação". Um processo matemático reversível claramente especificado usado para transformar dados de texto não criptografado em dados criptografados e vice-versa. Consulte *Criptografia Forte.*
Algoritmo de Encriptação	Consulte *Algoritmo de Criptografia*.
Análises de Risco Direcionada	Para fins do PCI DSS, uma análise de risco que se concentra em um ou mais requisito(s) específico(s) do PCI DSS de interesse, seja porque o requisito permite flexibilidade (por exemplo, quanto à frequência) ou, para a abordagem personalizada, para explicar como a entidade avaliou o risco e determinou que o controle personalizado atende ao objetivo de um requisito do PCI DSS.
ANSI	Acrônimo para "American National Standards Institute [Instituto Nacional Americano de Normas]".
Antimalware	Software projetado para detectar e remover, bloquear ou conter várias formas de software malicioso.

Termo	Definição
AOC	Acrônimo para “Atestado de Conformidade.” O AOC é o formulário oficial do PCI SSC para comerciantes e prestadores de serviços atestarem os resultados de uma avaliação do PCI DSS, conforme documentado em um Questionário de Autoavaliação (SAQ) ou Relatório de Conformidade (ROC).
Aplicação	Inclui todos os programas ou grupos de programas adquiridos, personalizados e sob medida, incluindo aplicativos internos e externos (por exemplo, web).
Aplicativo Web	Um aplicativo que geralmente é acessado por meio de um navegador web ou por serviços web. Os aplicativos Web podem estar disponíveis para Internet ou em uma rede interna privada.
Área Sensível	Uma área sensível é normalmente um subconjunto do CDE e é qualquer área que abriga sistemas considerados críticos para o CDE. Isso inclui data centers, salas de servidores, salas de back-office em locais de varejo e qualquer área que concentre ou agregue dados do titular do cartão para armazenamento, processamento ou transmissão. As áreas sensíveis também incluem áreas contendo sistemas que gerenciam ou mantêm a segurança do CDE (por exemplo, aqueles que fornecem controles de segurança de rede ou que gerenciam a segurança física ou lógica). Isso exclui as áreas onde apenas terminais de ponto de venda estão presentes, como áreas de caixa em uma loja de varejo ou call centers onde os agentes estão recebendo pagamentos.
ASV	Acrônimo para “Approved Scanning Vendor [Fornecedor de Varredura Aprovado].” Empresa aprovada pelo PCI SSC para conduzir serviços de varredura de vulnerabilidade externa.
Autenticação	Processo de verificação da identidade de um indivíduo, dispositivo ou processo. A autenticação normalmente ocorre com um ou mais fatores de autenticação. Consulte *Conta*, *Credencial de Autenticação*, e *Fator de Autenticação*.
Autenticação Multifator	Método de autenticação de um usuário em que pelo menos dois fatores são verificados. Esses fatores incluem algo que o usuário possui (como um cartão inteligente ou dongle), algo que o usuário conhece (como uma senha, frase secreta ou PIN) ou algo que o usuário é ou faz (como impressões digitais e outros elementos biométricos).
Autorização	No contexto de controle de acesso, autorização é a concessão de acesso ou outros direitos a um usuário, programa ou processo. A autorização define o que um indivíduo ou programa pode fazer após uma autenticação bem-sucedida. No contexto de uma transação com cartão de pagamento, a autorização se refere ao processo de autorização, que termina quando um comerciante recebe uma resposta da transação (por exemplo, uma aprovação ou recusa).
Avaliação de Risco	Processo em toda a empresa que identifica recursos valiosos de sistema e ameaças; quantifica as exposições de perda (ou seja, potencial de perda) com base em frequências estimadas e custos de ocorrência; e (opcionalmente) recomenda como alocar recursos para contramedidas para minimizar a exposição total. Consulte *Análises de Risco Direcionada*.
Bandeira de Pagamento	Uma organização com cartões de pagamento de sua marca ou outras formas de cartão de pagamento. As bandeiras de pagamento regulam onde e como os cartões de pagamento ou outras formas com sua marca ou logotipo são usados. Uma bandeira de pagamento pode ser uma bandeira de pagamento participante do PCI SSC ou outra bandeira, esquema ou rede de pagamento global ou regional.

Termo	Definição
Bandeira de Pagamento Participante	Também conhecida como "bandeira de pagamento". Uma bandeira de cartão de pagamento que, na época em questão, foi formalmente admitida como (ou afiliada) um membro do PCI SSC de acordo com seus documentos regulamentares. No momento em que este artigo foi escrito, as bandeiras de pagamento participantes incluem membros fundadores e membros estratégicos do PCI SSC.
BAU	Acrônimo para “Business as Usual [Negócio habitual]”.
Bloco de PIN	Um bloco de dados usado para encapsular um PIN durante o processamento. O formato de bloco de PIN define o conteúdo do bloco de PIN e como ele é processado para recuperar o PIN. O bloco de PIN é composto pelo PIN, o comprimento do PIN e pode conter o PAN (ou um truncamento dele) dependendo do Formato ISO do Bloco de PIN usado.
Canal de Pagamento	Métodos utilizados por comerciantes para aceitar pagamentos dos clientes. Os canais de pagamento comuns incluem os cartão presente (em pessoa) e o cartão não presente (comércio eletrônico e MO/TO)
Cartões de Pagamento	Para fins de PCI DSS, qualquer forma de cartão de pagamento que tenha o logotipo de qualquer bandeira de pagamento participante do PCI SSC.
CDE	Acrônimo para “Cardholder Data Environment [Ambiente de Dados do Titular do Cartão]” O CDE é composto por: • Componentes de sistema, pessoas e processos que armazenam, processam e transmitem dados do titular do cartão ou dados de autenticação confidenciais ou, • Componentes de sistema que podem não armazenar, processar ou transmitir CHD/SAD, mas têm conectividade irrestrita aos componentes do sistema que armazenam, processam ou transmitem CHD/SAD.
CERT	Acrônimo para “Computer Emergency Response Team [Time de Resposta à Emergência Computacional].”
Chave Criptográfica	Um parâmetro usado em conjunto com um algoritmo de criptografia que é usado para operações como: • Transformar dados de texto não criptografado em dados de texto cifrado, • Transformar dados de texto cifrado em dados de texto não criptografado, • Gerar uma assinatura digital calculada a partir de dados, • Verificar uma assinatura digital calculada a partir de dados, • Um código de autenticação calculado a partir de dados, ou • Um acordo de troca de um segredo compartilhado. Consulte *Criptografia Forte.*
CIS	Acrônimo para “Center for Internet Security [Centro para Segurança de Internet].”
Classificação de Risco	Processo de classificação de riscos para identificar, priorizar e abordar itens em ordem de importância.

Termo	Definição
Codificação Segura	O processo de criação e implementação de aplicativos resistentes à adulteração e/ou comprometimento.
Código de Verificação do Cartão	Também conhecido como Código ou Valor de Validação do Cartão ou Código de Segurança do Cartão. Para fins de PCI DSS, é o valor de três ou quatro dígitos impresso na frente ou no verso de um cartão de pagamento. Pode ser referido como CAV2, CVC2, CVN2, CVV2 ou CID de acordo com as bandeiras de pagamento participantes. Para mais informações, entre em contato com as bandeiras de pagamento participantes.
Código de Serviço	Valor de três ou quatro dígitos na tarja magnética após a data de vencimento do cartão de pagamento na trilha de dados. É usado para várias coisas, como definir atributos de serviço, diferenciar entre intercâmbio internacional e nacional ou identificar restrições de uso.
Comercial de Prateleira (COTS)	Descrição dos produtos que são itens de estoque não especificamente customizados ou projetados para um cliente ou usuário específico e estão prontamente disponíveis para uso.
Comerciante	Para os fins do PCI DSS, um comerciante é definido como qualquer entidade que aceita cartões de pagamento com os logotipos de qualquer bandeira de pagamento participante do PCI SSC como pagamento por bens e/ou serviços. Um comerciante que aceita cartões de pagamento como pagamento por mercadorias e/ou serviços também pode ser um prestador de serviços, se os serviços vendidos resultarem no armazenamento, processamento ou transmissão de dados do titular do cartão em nome de outros comerciantes ou prestadores de serviços. Por exemplo, um ISP (provedor de serviços de Internet) é um comerciante que aceita cartões de pagamento para faturamento mensal, mas também é um prestador de serviços se hospedar comerciantes como clientes.
Componentes de Sistema	Quaisquer dispositivos de rede, servidores, dispositivos de computação, componentes virtuais ou software incluídos ou conectados ao CDE, ou que possam impactar na segurança do CDE.
Comprometimento	Também conhecido como "comprometimento de dados" ou "violação de dados". Intrusão em um sistema de computador onde houver suspeita de divulgação/roubo, modificação ou destruição não autorizada de dados do titular do cartão.
Conexão de Rede	Um caminho de comunicação lógico, físico ou virtual entre dispositivos que permite a transmissão e recepção de pacotes da camada de rede.
Conhecimento Dividido	Um método pelo qual duas ou mais entidades separadamente possuem componentes principais ou compartilhamentos de chaves que individualmente não transmitem nenhum conhecimento da chave criptográfica resultante.
Console	Tela e/ou teclado diretamente conectado que permite acesso e controle de um servidor, computador mainframe ou outro tipo de sistema. Consulte o *Acesso não-console*.
Consumidor	O titular do cartão que está adquirindo bens, serviços ou ambos.
Conta	Também conhecido como "ID do usuário", "ID da conta" ou "ID do aplicativo". Usado para identificar um indivíduo ou processo em um sistema de computador. Consulte *Credencial de Autenticação* e *Fator de Autenticação.*

Termo	Definição
Conta Padrão	Conta de login predefinida em um sistema, aplicativo ou dispositivo para permitir o acesso inicial quando o sistema é colocado em serviço pela primeira vez. Contas padrão adicionais também podem ser geradas pelo sistema como parte do processo de instalação.
Contas de Aplicativo e Sistema	Também chamadas de "contas de serviço". Contas que executam processos ou tarefas em um sistema de computador ou em um aplicativo. Essas contas geralmente têm privilégios elevados que são necessários para executar tarefas ou funções especializadas e não são contas normalmente usadas por um indivíduo.
Controle de Mudança	Processos e procedimentos para revisar, testar e aprovar alterações em sistemas e software para impacto antes da implementação.
Controle Duplo	Processo de uso de duas ou mais entidades separadas (geralmente pessoas) operando em conjunto para proteger funções ou informações confidenciais. Ambas as entidades são igualmente responsáveis pela proteção física de materiais envolvidos em transações vulneráveis. Nenhuma pessoa individualmente tem permissão para acessar ou usar os materiais (por exemplo, a chave criptográfica). Para processos manuais de geração, transporte, carregamento, armazenamento e recuperação de chaves, o controle duplo requer a divisão do conhecimento da chave entre as entidades. Consulte *Conhecimento Dividido*.
Controle de Acesso Físico	Mecanismos que limitam o acesso a um espaço físico ou ambiente apenas a pessoas autorizadas. Consulte *Controle de Acesso lógico*.
Controle de Acesso Lógico	Mecanismos que limitam a disponibilidade de informações ou recursos de processamento de informações apenas para pessoas ou aplicativos autorizados. Consulte *Controle de Acesso Físico.*
Controles de Compensação	Consulte os Apêndices B e C do PCI DSS.
Controles de Segurança de Rede (NSC)	Firewalls e outras tecnologias de segurança de rede que atuam como pontos de aplicação da política de rede. Os NSCs normalmente controlam o tráfego de rede entre dois ou mais segmentos de rede lógicos ou físicos (ou sub-redes) com base em políticas ou regras predefinidas.
Credencial de Autenticação	Combinação do ID do usuário ou ID da conta mais o(s) fator(es) de autenticação usado(s) para autenticar um indivíduo, dispositivo ou processo. Consulte *Conta* e *Fator de Autenticação.*
Criptografia	A transformação (reversível) de dados por um algoritmo criptográfico para produzir texto cifrado, ou seja, para ocultar o conteúdo de informação dos dados. Consulte *Criptografia Forte.*
Criptografia de Banco de Dados em Nível de Coluna	Técnica ou tecnologia (software ou hardware) para criptografar o conteúdo de uma coluna específica em um banco de dados versus o conteúdo completo de todo o banco de dados. Como alternativa, consulte *Criptografia de Disco* e *Criptografia em Nível de Arquivo*.
Criptografia de Disco	Técnica ou tecnologia (software ou hardware) para criptografar todos os dados armazenados em um dispositivo (por exemplo, um disco rígido ou unidade flash). Como alternativa, a Criptografia em nível de arquivo ou Criptografia de banco de dados em nível de coluna é usada para criptografar o conteúdo de arquivos ou colunas específicas.

Termo	Definição
Criptografia em Nível de Arquivo	Técnica ou tecnologia (software ou hardware) para criptografar o conteúdo completo de arquivos específicos. Como alternativa, consulte *Criptografia de Disco* e *Criptografia de Banco de Dados em Nível de Coluna*.
Criptografia Forte	A criptografia é um método para proteger os dados por meio de um processo de criptografia reversível e é uma base primitiva usada em muitos protocolos e serviços de segurança. A criptografia forte é baseada em algoritmos testados e aceitos pelo setor, juntamente com comprimentos de chave que fornecem um mínimo de 112 bits de força de chave efetiva e práticas de gerenciamento de chave adequadas. A força efetiva da chave pode ser menor do que o comprimento de 'bit' real da chave, o que pode levar a algoritmos com chaves maiores fornecer menos proteção do que algoritmos com tamanhos de chave reais menores, porém mais efetivos. *Recomenda-se que todas as novas implementações usem um mínimo de 128 bits de força de chave efetiva.* Exemplos de referências da indústria em algoritmos criptográficos e comprimentos de chave incluem: • *NIST Special Publication 800-57 Part 1*, • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018), and* • *ISO/IEC 18033 Encryption algorithms, and* • *ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*
Criptoperíodo	O intervalo de tempo durante o qual uma chave criptográfica pode ser usada para seu propósito definido. Frequentemente definido em termos do período durante o qual a chave está ativa e/ou a quantidade de texto cifrado que foi produzido pela chave e de acordo com as práticas recomendadas e diretrizes da indústria (por exemplo, *NIST Special Publication 800-57*).
Custodiante de Chave	Uma função em que uma(s) pessoa(s) é(são) confiada(s) e responsável(is) pela execução de funções de gerenciamento de chaves envolvendo chaves secretas e/ou privadas, compartilhamentos de chaves ou componentes chave em nome de uma entidade.
CVSS	Acrônimo para “Common Vulnerability Scoring System [Sistema de Pontuação de Vulnerabilidade Comum].” Consulte o *Guia do Programa ASV* para obter mais informações.
Dados da Conta	Os dados da conta consistem nos dados do titular do cartão e/ou dados de autenticação confidenciais. Consulte os *Dados do Titular do Cartão* e os *Dados de Autenticação Confidenciais*.
Dados de Autenticação Confidenciais (SAD, em inglês)	Informações relacionadas à segurança usadas para autenticar os titulares dos cartões e/ou autorizar transações com cartões de pagamento. Essas informações incluem, mas não se limitam a, códigos/valores de validação do cartão, dados de trilha completos (de tarja magnética ou equivalente em um chip), PINs e blocos de PIN.
Dados de Tarja Magnética	Consulte *Dados de Trilha*.
Dados de Texto Aberto	Dados não criptografados.

Termo	Definição
Dados do Titular do Cartão (CHD – *Cardholder Data, em inglês*)	No mínimo, os dados do titular do cartão consistem no PAN completo. Os dados do titular do cartão também podem aparecer na forma do PAN completo mais qualquer um dos seguintes: nome do titular do cartão, data de validade e/ou código de serviço. Consulte *Dados de Autenticação Confidenciais* para elementos de dados adicionais que podem ser transmitidos ou processados (mas não armazenados) como parte de uma transação de pagamento.
Dados de Trilha	Também conhecido como "dados de trilha completo" ou "dados de tarja magnética". Dados codificados na tarja magnética ou chip usados para autenticação e/ou autorização durante as transações de pagamento. Pode ser a imagem da tarja magnética em um chip ou os dados da trilha na tarja magnética.
Diagrama de Fluxo de Dados	Um diagrama que mostra como os dados fluem por meio de um aplicativo, sistema ou rede.
Diagrama de Rede	Um diagrama que mostra os componentes de sistema e as conexões em um ambiente de rede.
DMZ	Abreviatura de “zona desmilitarizada”. Sub-rede física ou lógica que fornece uma camada adicional de segurança para a rede privada interna de uma organização.
DNS	Acrônimo para “Domain Name System [Sistema de Nome de Domínio].”
ECC	Acrônimo para “Elliptic Curve Cryptography [Criptografia de Curva Elíptica].” Consulte *Criptografia Forte.*
Emissor	Também conhecido como "banco emissor" ou "instituição financeira emissora". Entidade que emite cartões de pagamento ou executa, facilita ou apoia serviços de emissão, incluindo, mas não se limitando a bancos emissores e processadores de emissores.
Entidade	Termo usado para representar a corporação, organização ou negócio que está passando por uma avaliação do PCI DSS.
Equipamento para Clonagem de Cartão de Credito	Um dispositivo físico, geralmente conectado a um dispositivo legítimo de leitura de cartão, projetado para capturar e/ou armazenar ilegitimamente as informações de um cartão de pagamento.
Escopo	Processo de identificação de todos os componentes de sistema, pessoas e processos a serem incluídos em uma avaliação do PCI DSS. Consulte a seção 4 do PCI DSS “Escopo dos Requisitos do PCI DSS”
Evento de Segurança	Uma ocorrência considerada por uma organização como tendo implicações de segurança em potencial para um sistema ou seu ambiente. No contexto do PCI DSS, os eventos de segurança identificam atividades suspeitas ou anômalas.

Termo	Definição
Fator de Autenticação	O elemento usado para provar ou verificar a identidade de um indivíduo ou processo em um sistema de computador. A autenticação normalmente ocorre com um ou mais 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. O ID (ou conta) e o fator de autenticação juntos são considerados credenciais de autenticação." Consulte *Conta* e *Credencial de Autenticação.*
Forma de Cartão de Pagamento	Inclui cartões de pagamento físicos, bem como dispositivos com funcionalidade que emula um cartão de pagamento para iniciar uma transação de pagamento. Exemplos de tais dispositivos incluem, mas não estão limitados a, smartphones, smartwatches, pulseiras de fitness, chaveiros e itens que se podem vestir, como joias.
Firewall	Tecnologia de hardware e/ou software que protege os recursos da rede contra acesso não autorizado. Um firewall permite ou nega o tráfego de computador entre redes com diferentes níveis de segurança com base em um conjunto de regras e outros critérios.
Forense	Também conhecido como "análise forense de computador". No que se refere à segurança da informação, a aplicação de ferramentas investigativas e técnicas de análise para reunir evidências de recursos de computador para determinar a causa do comprometimento dos dados. As investigações sobre o comprometimento dos dados de pagamento são normalmente conduzidas por um PCI Forensic Investigator (PFI).
FTP	Acrônimo para "File Transfer Protocol [Protocolo de Transferência de Arquivos]". Protocolo de rede usado para transferir dados de um computador para outro por meio de uma rede pública como a Internet. O FTP é amplamente visto como um protocolo inseguro porque as senhas e o conteúdo do arquivo são enviados desprotegidos e em texto não criptografado. O FTP pode ser implementado com segurança via SSH ou outra tecnologia.
Geração de Chave Criptográfica	A geração de chaves é uma das funções do gerenciamento de chaves. Os documentos a seguir fornecem orientações reconhecidas sobre a geração adequada de chaves: • *NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation* • *ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle* – 4.3 Key generation • *ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle* – 6.2 Key life cycle stages — Generation • *European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management* – 4.1.1 Key generation [para algoritmos simétricos] – 4.2.1 Key generation [para algoritmos assimétricos].

Termo	Definição
Gerenciamento de Chave Criptográfica	O conjunto de processos e mecanismos que suportam o estabelecimento e manutenção de chaves criptográficas, incluindo a substituição de chaves antigas por novas, conforme necessário.
Hash Criptográfico com Chave	Uma função de hashing que incorpora uma chave secreta gerada aleatoriamente para fornecer resistência a ataques de força bruta e integridade de autenticação secreta. Algoritmos de hash criptográficos com chave adequados incluem, mas não estão limitados a: HMAC, CMAC e GMAC, com uma força criptográfica efetiva de pelo menos 128 bits *(NIST SP 800-131Ar2).* Consulte o seguinte para obter mais informações sobre HMAC, CMAC e GMAC, respectivamente: *NIST SP 800-107r1, NIST SP 800-38B, e NIST SP 800-38D).* Consulte *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms* §5.3.
Hashing	Um método para proteger dados que os converte em um resumo de mensagem de comprimento fixo. O hash é uma função unilateral (matemática) em que um algoritmo não secreto recebe qualquer mensagem de comprimento arbitrário como entrada e produz uma saída de comprimento fixo (geralmente chamado de "código hash" ou "resumo da mensagem"). As funções de hash devem ter as seguintes propriedades: • É computacionalmente inviável determinar a entrada original dado apenas o código hash, • É computacionalmente inviável encontrar duas entradas que forneçam o mesmo código hash.
HSM	Acrônimo para "hardware security module [módulo de segurança de hardware]" ou "host security module [módulo de segurança de host]." Um dispositivo de hardware protegido fisicamente e logicamente que fornece um conjunto seguro de serviços criptográficos, usado para funções de gerenciamento de chaves criptográficas e/ou descriptografia de dados de conta.
IDS	Acrônimo para "intrusion-detection system [sistema de detecção de intrusão]."
Independência Organizacional	Uma estrutura organizacional que garante que não haja conflito de interesses entre a pessoa ou departamento que executa a atividade e a pessoa ou departamento que avalia a atividade. Por exemplo, os indivíduos que realizam avaliações são organizacionalmente separados da gestão do ambiente que está sendo avaliado.
IPS	Acrônimo para "intrusion prevention system [sistema de prevenção de intrusão]."
ISO	Acrônimo para "International Organization for Standardization [Organização Internacional para Padronização]."
LAN	Acrônimo para "local área network [rede de área local]."
LDAP	Acrônimo para "Lightweight Directory Access Protocol [Protocolo de Acesso ao Diretório de Peso Leve]."
Login Interativo	O processo de um indivíduo fornecer credenciais de autenticação para fazer logon diretamente em um aplicativo ou conta do sistema.

Termo	Definição
MAC	Em criptografia, um acrônimo para “message authentication code [código de autenticação de mensagem]”. Consulte *Criptografia Forte.*
Mascaramento	Método de ocultar um segmento do PAN quando exibido ou impresso. O mascaramento é usado quando não há necessidade de negócios para visualizar todo o PAN. O mascaramento está relacionado à proteção do PAN quando exibido em telas, recibos de papel, impressões, etc. Consulte *Truncamento* para proteção de PAN quando armazenado, processado ou transmitido eletronicamente.
Mídia Eletrônica Removível	Mídia que armazena dados digitalizados que podem ser facilmente removidos e/ou transportados de um sistema de computador para outro. Exemplos de mídia eletrônica removível incluem CD-ROM, DVD-ROM, unidades flash USB e discos rígidos externos/portáteis. Nesse contexto, a mídia eletrônica removível não inclui unidades hot-swappable, unidades de fita usadas para backups em massa ou outra mídia normalmente não usada para transportar dados de um local para uso em outro.
Mídias	Material físico, incluindo, mas não se limitando a, dispositivos de armazenamento eletrônico, mídia eletrônica removível e relatórios em papel.
MO/TO	Acrônimo para “Mail-Order/Telephone-Order [Pedido por telefone/correio]”.
Monitoramento de Integridade de Arquivo (FIM)	Uma solução de detecção de alterações que verifica as alterações, adições e exclusões em arquivos críticos e notifica quando tais alterações são detectadas.
NAC	Acrônimo para “Network Access Control [Controle de Acesso à Rede]”.
NAT	Acrônimo para “Network Address Translation [Tradução de Endereço de Rede]”.
NIST	Acrônimo para “National Institute of Standards and Technology [Instituto Nacional de Padrões e Tecnologia].” Agência federal não reguladora do Departamento de Comércio da Administração de Tecnologia nos EUA.
NTP	Acrônimo para “Network Time Protocol [Protocolo de Tempo de Rede]”.
Objeto de Nível de Sistema	Qualquer coisa em um componente de sistema que seja necessária para sua operação, incluindo, mas não se limitando a arquivos de configuração e executáveis de aplicativo, arquivos de configuração de sistema, bibliotecas estáticas e compartilhadas e DLLs, executáveis de sistema, drivers de dispositivo e arquivos de configuração de dispositivo e componentes de terceiros.
Oficial de Segurança	A principal pessoa responsável pela segurança de uma entidade.
OWASP	Acrônimo para “Open Web Application Security Project [Proteção de Segurança para Aplicações de Internet Aberta]”.

Termo	Definição
Página de Pagamento	Uma interface de usuário baseada na web que contém um ou mais elementos de formulário destinados a capturar dados de conta de um consumidor ou enviar dados de conta capturados. A página de pagamento pode ser processada como qualquer uma das seguintes: • Um único documento ou instância, • Um documento ou componente exibido em um "inline frame [quadro embutido]" em uma página de não pagamento, • Vários documentos ou componentes, cada um contendo um ou mais elementos de formulário contidos em vários "inline frames [quadros embutidos]" em uma página de não pagamento.
PAN	Acrônimo para "primary account number" [número da conta principal]. Número de cartão de pagamento exclusivo (cartões de crédito, débito ou pré-pagos, etc.) que identifica o emissor e a conta do titular do cartão.
Patch	Atualização do software existente para adicionar função ou corrigir um defeito.
PCI DSS	Acrônimo para "Payment Card Industry Data Security Standard [Padrão de Segurança de Dados da Indústria De Cartão de Pagamento]".
Pessoal	Funcionários em tempo integral e parcial, funcionários temporários, contratados e consultores com responsabilidades de segurança para proteger os dados da conta ou que podem afetar a segurança dos dados da conta.
PIN	Acrônimo para "Personal Identification Number [número de identificação pessoal]".
POI	Acrônimo para "Point of Interaction [ponto de interação]", o ponto inicial onde os dados são lidos de um cartão.
Sistema de Ponto de Vendas (POS, em inglês)	Hardware e Software utilizados por comerciantes para aceitar pagamentos dos clientes. Podem incluir dispositivos POI, Pads PIN, registros de dinheiro eletrônico, etc.
Prestador de Serviços	Entidade comercial que não é uma bandeira de pagamento, diretamente envolvida no processamento, armazenamento ou transmissão de dados do titular do cartão em nome de outra entidade. Isso inclui portais de pagamento, prestadores de serviços de pagamento (PSPs) e organizações de vendas independentes (ISOs). Isso também inclui empresas que prestam serviços que controlam ou poderiam impactar a segurança dos dados do titular do cartão. Os exemplos incluem prestadores de serviços gerenciados que fornecem firewalls gerenciados, IDS e outros serviços, assim como provedores de hospedagem e outras entidades. Se uma entidade fornece um serviço que envolve *apenas* o fornecimento de acesso à rede pública - como uma empresa de telecomunicações que fornece apenas o link de comunicação - a entidade não seria considerada um prestador para esse serviço (embora possam ser considerados um prestador para outros serviços). Consulte *Prestador de Serviços Multilocatário* e *Prestador de Serviços Terceirizado*.
Prestadores de Serviços Terceirizados (TPSP)	Qualquer terceiro agindo como um prestador de serviços em nome de uma entidade. Consulte *Prestador de Serviços Multilocatário* e *Prestador de Serviços*

Termo	Definição
Privilégios Mínimos	O nível mínimo de privilégios necessários para desempenhar as funções e responsabilidades da função de trabalho.
Processador de Pagamento	Algumas vezes é referido como "gateway de pagamento" ou "prestador de serviços de pagamento (PSP)". Entidade contratada por um estabelecimento comercial ou outra entidade para lidar com transações de cartões de pagamento em seu nome. Consulte *Adquirente*.
Prestador de Serviços Multilocatário	Um tipo de Prestador de Serviços Terceirizado que oferece vários serviços compartilhados com os comerciantes e outros prestadores de serviço, onde os clientes compartilham recursos do sistema (como servidores físicos ou virtuais), infraestrutura, aplicativos (incluindo software como serviço (SaaS)) e/ou bancos de dados. Os serviços podem incluir, mas não estão limitados a, hospedagem de múltiplas entidades em um único servidor compartilhado, prestação de serviço de comércio eletrônico e/ou “carrinho de compras”, serviços de hospedagem baseados na web, aplicativos de pagamento, vários aplicativos e serviços de nuvem e conexões com processadores e portais de pagamento. Consulte *Prestador de Serviços* e *Prestador de Serviços Terceirizados*.
QIR	Acrônimo para Qualified Integrator or Reseller [Revendedor ou Integrador Qualificado]”. Consulte o *Guia do Programa QIR* no site do PCI SSC para obter mais informações.
QSA	Acrônimo para “Qualified Security Assessor [Assessor de Segurança Qualificado]”. Os QSAs são qualificados pelo PCI SSC para realizar avaliações do PCI DSS no local. Consulte os *Requisitos de Qualificação do QSA* para obter detalhes sobre os requisitos para Empresas e Funcionários do QSA.
Rede Confiável	Rede de uma entidade que está dentro da capacidade da entidade de controlar ou gerenciar e que atenda aos requisitos aplicáveis do PCI DSS
Rede não Confiável	Qualquer rede que não atenda à definição de “rede confiável”.
Registro	Consulte o *Registro de Auditoria*.
Registro de Auditoria	Também conhecido como "trilha de auditoria". Registro cronológico das atividades do sistema. Fornece uma trilha verificável de forma independente suficiente para permitir a reconstrução, revisão e exame da sequência de ambientes e atividades que cercam ou conduzem à operação, procedimento ou evento em uma transação desde o início até os resultados finais.
ROC	Acrônimo para “Report on Compliance [Relatório de Conformidade]”. Relatório usado para documentar resultados detalhados da avaliação PCI DSS de uma entidade.
RSA	Algoritmo para codificação de chave pública. Consulte *Criptografia Forte.*
SAQ	Acrônimo para “Self-Assessment Questionnaire [Questionário de Autoavaliação]”. Relatório usado para documentar os resultados da autoavaliação do PCI DSS de uma entidade.

Termo	Definição
Scripts da Página de Pagamento	Quaisquer comandos ou instruções de linguagem de programação em uma página de pagamento que são processados e/ou interpretados pelo navegador de um consumidor, incluindo comandos ou instruções que interagem com o modelo de objeto de documento de uma página. Exemplos de linguagens de programação são JavaScript e VB script; nenhuma das linguagens de marcação (por exemplo, HTML) ou regras de estilo (por exemplo, CSS) são linguagens de programação.
Segmentação	Também conhecido como "segmentação de rede" ou "isolamento". A segmentação isola os componentes de sistemas que armazenam, processam ou transmitem os dados do titular do cartão dos sistemas que não o fazem. Consulte a seção 4 do PCI "Segmentação" na seção 4 do PCI DSS: *Requisitos.*
Senha / Frase Secreta	Uma sequência de caracteres que serve como fator de autenticação para um usuário ou conta.
Senha Padrão	Senha na administração do sistema, usuário ou contas de serviço predefinidas em um sistema, aplicativo ou dispositivo; geralmente associado à conta padrão. Contas e senhas padrão são publicadas e bem conhecidas e, portanto, facilmente adivinhadas.
Separação de Função	Prática de dividir as etapas em uma função entre vários indivíduos, para evitar que um único indivíduo subverta o processo.
Serviços de Emissão	Os exemplos de serviços de emissão incluem, mas não estão limitados a, autorização e personalização do cartão.
Servidor de redirecionamento de comércio eletrônico (web)	Um servidor que redireciona o navegador do cliente do site de um comerciante para um local diferente para processamento de pagamento durante uma transação de comércio eletrônico.
Sistema de Gestão de Chave	Uma combinação de hardware e software que fornece uma abordagem integrada para gerar, distribuir e / ou gerenciar chaves criptográficas para dispositivos e aplicativos.
Sistemas Críticos	Um sistema ou tecnologia que a entidade considera de particular importância. Por exemplo, um sistema crítico pode ser essencial para o desempenho de uma operação comercial ou para a manutenção de uma função de segurança. Exemplos de sistemas críticos geralmente incluem sistemas de segurança, dispositivos e sistemas voltados ao público, bancos de dados e sistemas que armazenam, processam ou transmitem dados do titular do cartão.
SNMP	Acrônimo para "Simple Network Management Protocol [Protocolo de Administração de Rede Simples]".
Software de Terceiros	Software adquirido por, mas não desenvolvido expressamente para uma entidade. Pode ser de código aberto, freeware, shareware ou adquirido.
Software sob Medida e Personalizado	*O software "bespoke [sob medida]"* é desenvolvido para a entidade por um terceiro em nome da entidade e de acordo com as especificações da entidade. *O software personalizado* é desenvolvido pela entidade para seu próprio uso.
SQL	Acrônimo para "Linguagem de Pesquisa Estruturada [Structured Query Language]".

Termo	Definição
SSH	Abreviatura de “Secure Shell [Concha de Segurança]”.
SSL	Acrônimo para “Secure Sockets Layer [Camadas de Sockets de Segurança]”.
TDES	Acrônimo para “Triple Data Encryption Standard [Padrão de Codificação Tripla de Dados]”. Também conhecido como "3DES" ou "Triple DES".
Telnet	Abreviatura de “telephone network protocol [protocolo de rede telefônica]”.
Terminal de Pagamento Virtual	No contexto do Questionário de Autoavaliação (SAQ) C-VT, um terminal de pagamento virtual é o acesso baseado em navegador da web a um adquirente, processador ou site de prestador de serviços terceirizados para autorizar transações de cartão de pagamento, onde o comerciante entra manualmente dados do cartão de pagamento por meio de um navegador da web. Ao contrário dos terminais físicos, os terminais de pagamento virtuais não leem dados diretamente de um cartão de pagamento. Como as transações de cartão de pagamento são inseridas manualmente, os terminais de pagamento virtuais são normalmente usados em vez de terminais físicos em ambientes comerciais com baixos volumes de transações.
Titular do Cartão	Cliente para o qual um cartão de pagamento é emitido ou qualquer indivíduo autorizado a usar o cartão de pagamento.
TLS	Acrônimo para “Transport Layer Security [Segurança da Camada de Transporte]”.
Token	No contexto de autenticação e controle de acesso, um token é um valor fornecido por hardware ou software que funciona com um servidor de autenticação ou VPN para executar funções dinâmicas ou multifatoriais.
Token de Índice	Um valor aleatório de uma tabela de valores aleatórios que corresponde a um determinado PAN.
Truncamento	Método de tornar um PAN totalmente ilegível, removendo um segmento de dados do PAN. O truncamento está relacionado à proteção do PAN quando armazenado, processado ou transmitido eletronicamente. Consulte *Mascaramento* para proteção de PAN quando exibido em telas, recibos de papel, etc.
Usuário Privilegiado	Qualquer conta de usuário com privilégios de acesso superiores aos básicos. Normalmente, essas contas têm privilégios elevados ou aumentados com mais direitos do que uma conta de usuário padrão. No entanto, a extensão dos privilégios em diferentes contas com privilégios pode variar muito, dependendo da organização, função ou função do trabalho e da tecnologia em uso.
Virtualização	A abstração lógica de recursos de computação de restrições físicas e/ou lógicas. Uma abstração comum é conhecida como máquinas virtuais ou VMs, que pega o conteúdo de uma máquina física e permite que ela opere em hardware físico diferente e/ou junto com outras máquinas virtuais no mesmo hardware físico. Outras abstrações comuns incluem, mas não estão limitadas a, contêineres, computação sem servidor ou microsserviços.
VPN	Acrônimo para “virtual private network [rede virtual privada].”
Vulnerabilidade	Falha ou fraqueza que, se explorada, pode resultar no comprometimento intencional ou não intencional de um sistema.