



# Indústria de cartões de pagamento (PCI) Padrão de Segurança de Dados

---

## Requisitos e procedimentos da avaliação de segurança

**Versão 3.2**  
**Abril de 2016**

### 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.*

## Alterações no documento

Data	Versão	Descrição	Páginas
Outubro de 2008	1.2	Introduzir PCI DSS v1.2 como “Requisitos do PCI DSS e dos procedimentos de avaliação da segurança”, eliminando a redundância entre os documentos e fazer mudanças gerais e específicas de Procedimentos de auditoria de segurança do PCI DSS v1.1. Para obter informações completas, consulte Resumo de alterações no padrão de segurança de dados do PCI do PCI DSS Versão 1.1 para 1.2.	
Julho de 2009	1.2.1	Adicionar sentença que foi excluída incorretamente entre o PCI DSS v1.1 e v1.2.	5
		Corrigir grafia nos procedimentos de teste 6.3.7.a e 6.3.7.b.	32
		Remover marca cinza nas colunas “implantado” e “não implantado” nos procedimentos de teste 6.5.b.	33
		Para a Planilha de controles de compensação – exemplo completo, corrigir o texto no alto da página para “Use esta planilha para definir os controles de compensação para qualquer requisito indicado como “implantado” via controles de compensação.”	64
Outubro de 2010	2.0	Atualizar e implementar as alterações da v1.2.1. Consulte <i>Resumo de alterações do – PCI DSS a partir da versão 1.2.1 para a 2.0 do PCI-DSS</i> .	
Novembro de 2013	3.0	Atualizar a partir da v2.0. Consulte <i>Resumo de alterações do – PCI DSS a partir da versão 2.0 para a 3.0 do PCI-DSS</i> .	
Abril de 2015	3.1	Atualizar da v3.0 do PCI DSS. Consulte <i>PCI DSS – Resumo das Alterações da versão 3.0 para 3.1 do PCI DSS</i> , para detalhes das alterações.	
Abril de 2016	3.2	Atualizar da v3.1 do PCI DSS. Consulte <i>PCI DSS – Resumo das Alterações da versão 3.1 para 3.2 do PCI DSS</i> , para detalhes das alterações.	

# Índice

<b>Alterações no documento .....</b>	<b>2</b>
<b>Introdução e visão geral do padrão de segurança de dados do PCI.....</b>	<b>5</b>
<i>Recursos PCI DSS.....</i>	<i>6</i>
<b>Informações de aplicabilidade do PCI DSS.....</b>	<b>7</b>
<b>Relação entre PCI DSS e PA-DSS .....</b>	<b>9</b>
<i>Aplicabilidade do PCI DSS para aplicativos PA-DSS .....</i>	<i>9</i>
<i>Aplicabilidade do PCI DSS para fornecedores de aplicativos de pagamento .....</i>	<i>9</i>
<b>Escopo dos requisitos do PCI DSS .....</b>	<b>10</b>
<i>Segmentação da rede .....</i>	<i>11</i>
<i>Sem fio .....</i>	<i>12</i>
<i>Uso dos prestadores de serviços terceirizados/terceirização .....</i>	<i>12</i>
<b>Melhores práticas para implementar o PCI DSS nos processos de cenários de referência .....</b>	<b>13</b>
<b>Para os assessores: Amostragem de áreas de negócios e componentes do sistema.....</b>	<b>15</b>
<b>Controles de compensação .....</b>	<b>16</b>
<b>Instruções e conteúdo para o relatório sobre conformidade .....</b>	<b>17</b>
<b>Processo de avaliação do PCI DSS .....</b>	<b>17</b>
<b>Versões do PCI DSS .....</b>	<b>18</b>
<b>Requisitos detalhados do PCI DSS e procedimentos da avaliação de segurança.....</b>	<b>19</b>
<b>Construir e manter a segurança de rede e sistemas.....</b>	<b>20</b>
<i>Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão .....</i>	<i>20</i>
<i>Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança .....</i>	<i>29</i>
<b>Proteger os dados do titular do cartão .....</b>	<b>37</b>
<i>Requisito 3: Proteger os dados armazenados do titular do cartão .....</i>	<i>37</i>
<i>Requisito 4: Criptografar a transmissão de dados do titular do cartão em redes abertas e públicas.....</i>	<i>52</i>
<b>Manter um programa de gerenciamento de vulnerabilidades .....</b>	<b>55</b>
<i>Requisito 5: Proteja todos os sistemas contra softwares prejudiciais e atualize regularmente programas ou software de antivírus .....</i>	<i>55</i>
<i>Requisito 6: Desenvolver e manter sistemas e aplicativos seguros .....</i>	<i>59</i>
<b>Implementar medidas rigorosas de controle de acesso .....</b>	<b>76</b>
<i>Requisito 7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio .....</i>	<i>76</i>

<i>Requisito 8:</i>	<i>Identifique e autentique o acesso aos componentes do sistema .....</i>	<i>79</i>
<i>Requisito 9:</i>	<i>Restringir o acesso físico aos dados do titular do cartão.....</i>	<i>91</i>
<b>Monitorar e testar as redes regularmente.....</b>		<b>101</b>
<i>Requisito 10:</i>	<i>Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão .....</i>	<i>101</i>
<i>Requisito 11:</i>	<i>Testar regularmente os sistemas e processos de segurança.....</i>	<i>111</i>
<b>Manter uma política de segurança de informações.....</b>		<b>121</b>
<i>Requisito 12:</i>	<i>Mantenha uma política que aborde a segurança da informação para todas as equipes. ....</i>	<i>121</i>
<b>Apêndice A: Requisitos adicionais do PCI DSS .....</b>		<b>134</b>
<i>Apêndice A1:</i>	<i>Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada.....</i>	<i>135</i>
<i>Apêndice A2:</i>	<i>Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS .....</i>	<i>137</i>
<i>Apêndice A3:</i>	<i>Validação Suplementar de Entidades Designadas (DESV) .....</i>	<i>140</i>
<b>Apêndice B: Controles de compensação.....</b>		<b>157</b>
<b>Apêndice C: Planilha dos controles de compensação .....</b>		<b>159</b>
<b>Apêndice D: Segmentação e amostragem de áreas de negócios/componentes do sistema.....</b>		<b>162</b>

## Introdução e visão geral do padrão de segurança de dados do PCI

O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) foi desenvolvido para incentivar e aprimorar a segurança dos dados do titular do cartão e promover a ampla adoção de medidas de segurança de dados consistentes no mundo todo. O PCI DSS oferece a base de requisitos técnicos e operacionais elaborados para proteger os dados da conta. O PCI DSS aplica-se a **todas** as entidades envolvidas nos processos de pagamento do cartão — inclusive comerciantes, processadores, adquirentes, emissores e prestadores de serviço. O PCI DSS também se aplica a **todas** as outras entidades que armazenam, processam ou transmitem dados do titular do cartão (CHD) e/ou dados de autenticação confidenciais (SAD). Abaixo, há uma visão geral de alto nível dos 12 requisitos do PCI DSS.

### Padrão de segurança de dados do PCI – Visão geral alto nível

<b>Construir e manter a segurança de rede e sistemas</b>	<ol style="list-style-type: none"> <li>1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão</li> <li>2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança</li> </ol>
<b>Proteger os dados do titular do cartão</b>	<ol style="list-style-type: none"> <li>3. Proteger os dados armazenados do titular do cartão</li> <li>4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas</li> </ol>
<b>Manter um programa de gerenciamento de vulnerabilidades</b>	<ol style="list-style-type: none"> <li>5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus</li> <li>6. Desenvolver e manter sistemas e aplicativos seguros</li> </ol>
<b>Implementar medidas rigorosas de controle de acesso</b>	<ol style="list-style-type: none"> <li>7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio</li> <li>8. Identificar e autenticar o acesso aos componentes do sistema</li> <li>9. Restringir o acesso físico aos dados do titular do cartão</li> </ol>
<b>Monitorar e testar as redes regularmente</b>	<ol style="list-style-type: none"> <li>10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão</li> <li>11. Testar regularmente os sistemas e processos de segurança</li> </ol>
<b>Manter uma política de segurança de informações</b>	<ol style="list-style-type: none"> <li>12. Manter uma política que aborde a segurança da informação para todas as equipes</li> </ol>

Este documento, *Requisitos dos Padrão de Segurança de Dados do PCI e Procedimentos de Avaliação da Segurança*, usa como base os 12 requisitos do PCI DSS e combina-os com procedimentos de testes correspondentes em uma ferramenta de avaliação de segurança. Ele foi projetado para o uso durante as avaliações de conformidade PCI DSS como parte do processo de validação de uma entidade. As seguintes seções oferecem orientações e as práticas recomendadas para auxiliar entidades a conduzir, relatar e se preparar para os resultados de uma avaliação PCI DSS. Os requisitos e procedimentos de teste do PCI DSS se iniciam na página 15.

O PCI DSS compreende um conjunto mínimo de requisitos para proteger os dados da conta e pode ser aperfeiçoado por controles e práticas adicionais para amenizar ainda mais os riscos, bem como as normas e leis locais, regionais e do setor. Além disso, os requisitos legais ou regulatórios podem exigir proteção específica para informações pessoais ou outros elementos de dados (por exemplo, o nome do titular do cartão). O PCI DSS não substitui as leis locais ou regionais, normas governamentais ou outros requisitos legais.

## **Recursos PCI DSS**

O site do PCI Security Standards Council (PCI SSC) ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) contém alguns recursos adicionais para auxiliar as organizações com suas avaliações e validações do PCI DSS, inclusive:

- Biblioteca de documentos, incluindo:
  - *PCI DSS – Resumo de alterações a partir da versão 2.0 para a 3.0 do PCI-DSS*
  - *Guia de referência rápida do PCI DSS*
  - *Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS*
  - *Suplementos informativos e orientações*
  - *Abordagem priorizada para o PCI DSS*
  - *Relatório de conformidade (ROC) Modelo de relatório e Instruções de relatório*
  - *Questionários de autoavaliação (SAQs) e diretrizes e instruções do SAQ*
  - *Atestados de conformidade (AOCs)*
- Perguntas frequentes (FAQs)
- PCI para sites de pequenos comerciantes
- Treinamentos e seminários online do PCI
- Lista de assessores de segurança qualificados (QSAs) e fornecedores de varredura aprovados (ASVs)
- Lista de dispositivos PTS aprovados e aplicativos PA-DSS de pagamento validados

**Observação:** Os suplementos informativos complementam o PCI DSS e identificam considerações adicionais e recomendações para atender aos requisitos do PCI DSS—eles não alteram, eliminam ou sobrepõem o PCI DSS ou qualquer de seus requisitos.

Consulte [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) para obter informações sobre estes e outros recursos.

## Informações de aplicabilidade do PCI DSS

O PCI DSS aplica-se a **todas** as entidades envolvidas nos processos de pagamento do cartão — inclusive comerciantes, processadores, adquirentes, emissores e prestadores de serviço. O PCI DSS também se aplica a **todas** as outras entidades que armazenam, processam ou transmitem dados do titular do cartão e/ou dados de autenticação confidenciais.

Os dados do titular do cartão e os dados de autenticação confidenciais são definidos conforme segue:

Dados contábeis	
Os dados do titular do cartão incluem:	Os dados de autenticação confidenciais incluem:
<ul style="list-style-type: none"> <li>▪ O número da conta principal (PAN)</li> <li>▪ Nome do titular do cartão</li> <li>▪ Data de vencimento</li> <li>▪ Código de serviço</li> </ul>	<ul style="list-style-type: none"> <li>▪ Dados de rastreamento completo (dados em tarja magnética ou equivalentes em chip)</li> <li>▪ CAV2/CVC2/CVV2/CID</li> <li>▪ PINs/Bloqueios de PIN</li> </ul>

**O primeiro número contábil é o fator determinante para os dados do titular do cartão.** Se o nome, código de serviço e/ou data de validade do titular do cartão são armazenados, processados ou transmitidos com o PAN ou, de outro modo, estão presentes no ambiente de dados do titular do cartão (CDE), eles devem ser protegidos de acordo com os requisitos aplicáveis do PCI DSS.

Os requisitos do PCI DSS aplicam-se a organizações onde os dados da conta (dados do titular do cartão e/ou dados de autenticação confidenciais) são armazenados, processados ou transmitidos. Alguns requisitos do PCI DSS também podem ser aplicáveis a organizações que tenham terceirizado suas operações de pagamento ou o gerenciamento de seu CDE<sup>1</sup>. Além disso, as organizações que terceirizam seu CDE ou operações de pagamento para terceiros são responsáveis por garantir que os dados contábeis sejam protegidos por este terceiro conforme os requisitos aplicáveis do PCI DSS.

A tabela a seguir ilustra os elementos comumente usados do titular do cartão e dados de autenticação confidenciais, se o armazenamento de cada elemento de dados é permitido ou proibido e se cada elemento de dados deve ser protegido. Essa tabela não é completa, mas é exibida para ilustrar os diferentes tipos de requisitos que se aplicam a cada elemento de dados.

<sup>1</sup> De acordo com os programas em conformidade com a empresa de pagamento individual

		Elemento de dados	Armazenamento permitido	Converter dados armazenados ilegíveis conforme Requisito 3.4
<b>Dados contábeis</b>	<b>Dados do titular do cartão</b>	O número da conta principal (PAN)	Sim	Sim
		Nome do titular do cartão	Sim	Não
		Código de serviço	Sim	Não
		Data de vencimento	Sim	Não
	<b>Dados de autenticação confidenciais<sup>2</sup></b>	Dados de rastreamento completo <sup>3</sup>	Não	Não armazenável conforme Requisito 3.2
		CAV2/CVC2/CVV2/CID <sup>4</sup>	Não	Não armazenável conforme Requisito 3.2
		PIN/Bloco de PIN <sup>5</sup>	Não	Não armazenável conforme Requisito 3.2

Os Requisitos 3.3 e 3.4 do PCI DSS aplicam-se apenas ao PAN. Se o PAN for armazenado com outros elementos dos dados do titular do cartão, somente o PAN deverá ser convertido como ilegível de acordo com o Requisito 3.4 do PCI DSS.

Dados de autenticação confidenciais não devem ser armazenados após a autorização, mesmo se forem criptografados. Isso se aplica mesmo onde não há PAN no ambiente. As organizações devem entrar em contato diretamente com seu adquirente ou empresa de pagamento para saber se é permitido armazenar o SAD antes da autorização, por quanto tempo e quaisquer requisitos de proteção e utilização.

<sup>2</sup> Os dados de autenticação confidenciais não devem ser armazenados após a autorização (mesmo se forem criptografados).

<sup>3</sup> Dados de rastreamento completo da tarja magnética, dados equivalentes no chip, ou em outro lugar

<sup>4</sup> O valor de três ou quatro dígitos impresso na frente ou atrás de um cartão de pagamento

<sup>5</sup> Número de identificação pessoal inserido pelo titular do cartão durante uma transação com cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação

## Relação entre PCI DSS e PA-DSS

### ***Aplicabilidade do PCI DSS para aplicativos PA-DSS***

O uso de um aplicativo compatível com o Padrão de Segurança de Dados de Formulário de Pagamento (PA-DSS) não torna uma entidade compatível com o PCI DSS por si só, uma vez que o aplicativo deve ser implementado em um ambiente compatível com o PCI DSS e de acordo com o Guia de implementação do PA-DSS oferecido pelo fornecedor do aplicativo de pagamento.

Todos os aplicativos que armazenam, processam ou transmitem dados do titular do cartão abrangem uma avaliação do PCI DSS da entidade, incluindo aplicativos que tenham sido validados para PA-DSS. A avaliação do PCI DSS deve verificar se o aplicativo de pagamento validado do PA-DSS está configurado adequadamente e implementado com segurança conforme os requisitos do PCI DSS. Se o aplicativo de pagamento tiver passado por qualquer customização, uma revisão mais detalhada será exigida durante a avaliação do PCI DSS, já que o aplicativo pode não ser mais característico da versão que foi validada para o PA-DSS.

Os requisitos do PA-DSS derivam-se dos *Requisitos do PCI DSS e dos procedimentos de avaliação da segurança* (definidos neste documento). O PA-DSS detalha os requisitos que um aplicativo de pagamento deve atender para facilitar a conformidade do PCI DSS de um cliente. Uma vez que as ameaças à segurança evoluem constantemente, os aplicativos que já não contam com o suporte do fornecedor (por exemplo, identificados pelo vendedor como "fim da vida útil") não podem oferecer o mesmo nível de segurança das versões para as quais há suporte.

Os aplicativos de pagamento seguro, quando implementados em um ambiente compatível com PCI-DSS, minimizarão as possibilidades de quebras na segurança, levando ao comprometimento do PAN, dados de rastreamento completo, códigos e valores de validação do cartão (CAV2, CID, CVC2 e CVV2), PINs e bloqueios de PIN e a fraudes destruidoras resultantes dessas quebras.

Para determinar se o PA-DSS se aplica a um determinado aplicativo de pagamento, consulte o Guia do programa PA-DSS que pode ser encontrado no site [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

### ***Aplicabilidade do PCI DSS para fornecedores de aplicativos de pagamento***

O PCI DSS pode se aplicar a fornecedores de aplicativos de pagamentos se estes armazenam, processam ou transmitem dados do titular do cartão, ou se tiverem acesso aos dados do titular do cartão de seus clientes (por exemplo, na função de um prestador de serviços).

## Escopo dos requisitos do PCI DSS

Os requisitos de segurança do PCI DSS se aplicam a todos os componentes do sistema que estejam incluídos ou conectados no ambiente dos dados do titular do cartão. O ambiente de dados do titular do cartão (CDE) compreende pessoas, processos e tecnologias que armazenam, processam, ou transmitem os dados do titular do cartão ou dados de autenticação confidenciais. Os “componentes do sistema” incluem dispositivos de rede, servidores, dispositivos de computação e aplicativos. Exemplos de componentes do sistema incluem, entre outros, o seguinte:

- Sistemas que oferecem serviços de segurança (por exemplo, servidores de autenticação), facilitam a segmentação (por exemplo, firewalls internos) ou podem impactar a segurança do CDE (por exemplo, servidores de redirecionamento de rede ou resolução de nome).
- Componentes de virtualização como máquinas virtuais, switches/roteadores virtuais, mecanismos virtuais, aplicativos/desktops virtuais e hipervisores.
- Os componentes de rede incluem, entre outros, firewalls, switches, roteadores, pontos de acesso sem fio, dispositivos de rede e outros dispositivos de segurança.
- Os tipos de servidor incluem, entre outros, Web, aplicativo, banco de dados, autenticação, e-mail, proxy, NTP (Network Time Protocol) e DNS (Domain Name Server).
- Os aplicativos incluem todos os aplicativos adquiridos e personalizados, incluindo os aplicativos internos e externos (internet, por exemplo).
- Qualquer outro componente ou dispositivo interno ou conectado ao CDE.

A primeira etapa de uma avaliação do PCI DSS é determinar precisamente o escopo da revisão. Ao menos anualmente e antes da avaliação anual, a entidade avaliada deve confirmar a precisão do seu escopo no PCI DSS identificando todos os locais e fluxos de dados do titular do cartão, bem como identificar todos os sistemas a ele conectados ou, se comprometidos, que poderiam impactar o CDE (por exemplo, servidores de autenticação), para garantir que estejam incluídos no escopo do PCI DSS. Todos os tipos de sistemas e locais devem ser considerados parte do processo no escopo, inclusive sites de backup/recuperação e sistemas de transferência automática por falha.

Para confirmar a precisão do CDE definido, proceda conforme a seguir:

- A entidade avaliada identifica e documenta a existência de todos os dados do titular do cartão em seu ambiente, para verificar se nenhum dado do titular do cartão existe fora do CDE definido no momento.
- Assim que todos os locais dos dados do titular do cartão forem identificados e documentados, a entidade usa os resultados para verificar se o escopo do PCI DSS é adequado (por exemplo, os resultados podem ser um diagrama ou um inventário de locais de dados do titular do cartão).
- A entidade considera que quaisquer dados do titular do cartão encontrados estão no escopo da avaliação do PCI DSS e são parte do CDE. Se a entidade identificar dados que não estejam atualmente incluídos no CDE, estes dados devem ser apagados com segurança, migrados para o CDE definido atualmente ou para o CDE redefinido para incluir estes dados.

A entidade retém a documentação que mostra como o escopo do PCI DSS foi determinado. A documentação é retida para a revisão da assessoria e/ou para referência durante a próxima atividade anual de confirmação do escopo do PCI DSS.

Para cada avaliação do PCI DSS, é necessário que o assessor valide que o escopo da avaliação está corretamente definido e documentado.

### **Segmentação da rede**

A segmentação da rede ou o isolamento (separação) do ambiente de dados do titular do cartão do restante da rede corporativa não é um requisito do PCI DSS. Entretanto, ela é recomendada como um método que pode reduzir:

- O escopo da avaliação do PCI DSS
- O custo da avaliação do PCI DSS
- O custo e a dificuldade de implementar e manter controles do PCI DSS
- O risco de uma empresa (reduzido pela consolidação dos dados do titular do cartão em locais mais controlados e que totalizam um número menor)

Sem a segmentação adequada da rede (às vezes chamada de “rede plana”), toda a rede está no escopo da avaliação do PCI DSS. A segmentação da rede pode ser realizada por meio de firewalls internos da rede, roteadores com listas de controle de acesso rigorosas ou outras tecnologias que restringem o acesso a um determinado segmento de uma rede. Para ser considerado fora do escopo para o PCI DSS, um componente de sistema deve estar adequadamente isolado (segmentado) do CDE, de forma que mesmo se o componente de sistema fora do escopo estivesse comprometido, ele não poderia impactar na segurança do CDE.

Um pré-requisito importante para reduzir o escopo do ambiente de dados do titular do cartão é uma compreensão clara das necessidades do negócio e dos processos relacionados ao armazenamento, processamento ou transmissão dos dados do titular do cartão. Restringir os dados do titular do cartão à menor quantidade de locais possível ao eliminar dados desnecessários e consolidar os dados necessários talvez exija a reformulação de práticas de negócios de longa data.

Documentar os fluxos dos dados do titular do cartão por meio de um diagrama de fluxo de dados ajuda a compreender totalmente todos os fluxos de dados do titular do cartão e assegura que qualquer segmentação de rede seja eficiente no isolamento do ambiente de dados do titular do cartão.

Se a segmentação da rede tiver sido implementada e sendo usada para reduzir o escopo da avaliação do PCI DSS, o assessor deverá verificar se a segmentação é adequada para diminuir o escopo da avaliação. Em um nível elevado, a segmentação adequada da rede isola os sistemas que armazenam, processam ou transmitem dados do titular do cartão dos outros sistemas. Entretanto, a adequação de uma implementação específica da segmentação da rede varia muito e depende de certos fatores, como uma determinada configuração de rede, das tecnologias implementadas e de outros controles que podem ser empregados.

*Apêndice D: A segmentação e a amostragem dos componentes de sistema/áreas de negócio oferece mais informações sobre o efeito da segmentação e da amostragem da rede no escopo das avaliações do PCI DSS.*

## **Sem fio**

Se uma tecnologia sem fio for usada para armazenar, processar ou transmitir dados do titular do cartão (por exemplo, transações do ponto de venda, “quebra de linha”) ou se uma WLAN (Wireless Local Area Network) for parte do ou estiver conectada ao ambiente de dados do titular do cartão, os requisitos do PCI DSS e os procedimentos de teste para ambientes sem fio se aplicarão e deverão ser realizados (por exemplo, Requisitos 1.2.3, 2.1.1 e 4.1.1). Antes da tecnologia sem fio ser implementada, uma entidade deve avaliar cuidadosamente a necessidade da tecnologia com relação ao risco. Considere a implementação da tecnologia sem fio somente para a transmissão de dados não confidenciais.

## **Uso dos prestadores de serviços terceirizados/terceirização**

Um prestador de serviços ou comerciante pode usar um provedor terceirizado para armazenar, processar ou transmitir dados do titular do cartão em seu nome ou gerenciar componentes como roteadores, firewalls, bancos de dados, segurança física e/ou servidores. Se for o caso, talvez haja um impacto na segurança do ambiente de dados do titular do cartão.

As partes devem identificar claramente os serviços e componentes do sistemas que são incluídos no escopo da avaliação do PCI DSS do prestador de serviços, os requisitos específicos do PCI DSS abrangidos pelo prestador de serviços e quaisquer requisitos que os clientes do prestador de serviços sejam responsáveis por incluir em suas próprias revisões do PCI DSS. Por exemplo, um provedor de hospedagem gerenciada deve definir claramente quais endereços IP são mapeados como parte do seu processo trimestral de varredura de vulnerabilidade e por quais endereços IP os clientes são responsáveis na execução das varreduras trimestrais.

Os prestadores de serviços são responsáveis por demonstrar a conformidade do PCI DSS e podem ser obrigados a fazê-lo, conforme exigência das marcas sistemas de pagamento. Os prestadores de serviços devem entrar em contato com o adquirente e/ou marca do sistema de pagamento para determinar a validação de conformidade adequada.

Há duas opções para que os prestadores de serviços terceirizados comprovem a conformidade:

- 1) **Avaliação anual:** Os prestadores de serviços podem ser submetidos a avaliação(ões) do PCI DSS por conta própria e fornecer evidências aos clientes para comprovar a conformidade; ou
- 2) **Diversas avaliações sob demanda:** Se as avaliações do PCI DSS não forem realizadas por conta própria, os prestadores de serviços devem passar por avaliações mediante a solicitação dos clientes e/ou participar de cada avaliação do PCI DSS realizada pelos clientes, fornecendo os resultados de cada avaliação executada ao(s) respectivo(s) cliente(s)

Se o terceiro realizar sua própria avaliação do PCI DSS, ele deve fornecer evidências suficientes aos seus clientes para certificar que o escopo da avaliação do PCI DSS do prestador de serviços incluiu os serviços aplicáveis ao cliente e que os requisitos relevantes do PCI DSS foram examinados e determinados como adequados. O tipo específico de evidência fornecida pelo prestador de serviços aos seus clientes dependerá dos acordos/contratos em vigor entre as partes. Por exemplo, fornecer o AOC e/ou seções relevantes do ROC do prestador de serviços (redigido para proteger qualquer informação confidencial) pode ajudar a fornecer toda ou alguma informação.

Além disso, os comerciantes e prestadores de serviços devem gerenciar e monitorar a conformidade do PCI DSS de todos os terceiros associados quanto ao acesso aos dados do titular do cartão. *Para obter detalhes, consulte o Requisito 12.8 nesse documento.*

## Melhores práticas para implementar o PCI DSS nos processos de cenários de referência

Para assegurar que os controles de segurança continuem a ser adequadamente implementados, o PCI DSS deve ser implementado nas atividades do cenário de referência BAU (Business-As-Usual) como parte de uma estratégia global de segurança da entidade. Isso possibilita que uma entidade monitore a efetividade de seus controles de segurança continuamente e mantenha seu ambiente compatível com o PCI DSS entre as avaliações do PCI DSS. Exemplos de como incorporar o PCI DSS às atividades BAU incluem, entre outros:

1. Monitoramento de controles de segurança (como firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), monitoramento da integridade do arquivo (FIM), antivírus, controles de acesso, etc.) para assegurar que eles estejam funcionando de maneira efetiva e conforme o planejado.
2. Assegurar que todas as falhas nos controles de segurança sejam detectadas e resolvidas em tempo hábil. Os processos para resolver falhas no controle de segurança devem incluir:
  - Restaurar o controle de segurança
  - Identificar a causa da falha
  - Identificar e encaminhar quaisquer problemas de segurança que surgirem durante a falha do controle de segurança
  - Implementar a minimização (como controles técnicos ou de processo) para prevenir que a causa da falha ocorra novamente
  - Retomar o monitoramento do controle de segurança, talvez com monitoramento aprimorado por um período de tempo, para confirmar que o controle esteja funcionando de maneira efetiva
3. Revisar alterações no ambiente (por exemplo, acréscimo de novos sistemas, mudanças nas configurações de rede ou no sistema) antes de concluir a alteração e proceder conforme segue:
  - Determinar o possível impacto ao escopo do PCI DSS (por exemplo, uma nova regra do firewall que permite a conectividade entre um sistema no CDE e outro sistema pode trazer redes ou sistemas adicionais ao escopo para o PCI DSS).
  - Identificar os requisitos do PCI DSS aplicáveis aos sistemas e redes afetados pelas alterações (por exemplo, se um novo sistema estiver no escopo para o PCI DSS, será preciso configurá-lo de acordo com os padrões de configuração de sistema, incluindo FIM, AV, patches, registros de auditoria, etc. e será preciso adicioná-lo à programação trimestral de varredura de vulnerabilidade).
  - Atualizar o escopo do PCI DSS e implementar controles de segurança, conforme o caso.
4. Alterações na estrutura organizacional (por exemplo, aquisição ou fusão de uma empresa) que resultam em revisão formal do impacto ao escopo e requisitos do PCI DSS.
5. Comunicações e revisões periódicas para confirmar que os requisitos do PCI DSS permanecem em vigor e que os funcionários estão seguindo processos seguros. Estas revisões periódicas devem abranger todas as instalações e locais, incluindo pontos de venda, centros de dados, etc. e incluir a revisão dos componentes do sistema (ou amostras dos componentes do sistema), para garantir que os requisitos do PCI DSS continuem em vigor, por exemplo, os padrões de configuração foram aplicados, patches e AV estão atualizados, logs de

auditoria estão sendo revisados e assim por diante. A frequência das revisões periódicas deve ser determinada pela entidade conforme o tamanho e complexidade de seu ambiente.

Estas revisões também podem ser usadas para verificar se a evidência adequada está sendo mantida (por exemplo, logs de auditoria, relatórios de varredura de vulnerabilidade, revisões do firewall, etc.) a fim de auxiliar a preparação da entidade para sua próxima avaliação de conformidade.

6. Revisar tecnologias do software e hardware, pelo menos, uma vez ao ano para confirmar que continuam com suporte do fornecedor e podem atender aos requisitos de segurança da entidade, inclusive em relação ao PCI DSS. Se for constatado que as tecnologias não têm mais suporte do fornecedor ou não possam atender às necessidades de segurança da entidade, esta deve preparar um plano de retificação, atualizando e incluindo substituição da tecnologia, se necessário.

Além das práticas mencionadas acima, as organizações também podem querer considerar a implementação da separação de obrigações para suas funções de segurança para que as funções de auditoria e/ou segurança sejam separadas das funções operacionais. Em ambientes em que um indivíduo executa diversas funções (por exemplo, operações de segurança e administrativas), as obrigações podem ser atribuídas de forma que nenhum indivíduo possua controle total de um processo sem um ponto de verificação independentemente. Por exemplo, as responsabilidades pela configuração e responsabilidades pela aprovação de alterações podem ser atribuídas a indivíduos separados.

**Observação:** *Para algumas entidades, as práticas recomendadas pelo setor servem também como requisito para garantir a conformidade contínua do PCI DSS. Por exemplo, o PCI DSS inclui estes princípios em alguns requisitos e a Validação Suplementar de Entidades Designadas (PCI DSS, Apêndice A3) exige que entidades designadas procedam à validação destes princípios.*

*Todas as organizações devem considerar a implementação das práticas recomendadas no seu ambiente, mesmo onde a organização não é obrigada a validá-los.*

## Para os assessores: Amostragem de áreas de negócios e componentes do sistema

A amostragem é uma opção para que os assessores facilitem o processo de avaliação onde houver grandes números de áreas de negócios e/ou componentes do sistema.

Enquanto é aceitável que um assessor tire amostras das instalações do negócio/componentes do sistema como parte de sua revisão da conformidade do PCI DSS de uma entidade, não é aceitável que uma entidade aplique os requisitos do PCI DSS para apenas uma amostra de seu ambiente (por exemplo, requisitos de varredura trimestral de vulnerabilidade se aplicam a todos os componentes do sistema). Da mesma forma, não é aceitável que um assessor faça a revisão de apenas uma amostra dos requisitos do PCI DSS para analisar a conformidade.

Após considerar o escopo e a complexidade gerais do ambiente a ser avaliado, o assessor pode selecionar amostras representativas de áreas de negócios/componentes de sistema independentemente para avaliar a conformidade da entidade com os requisitos do PCI DSS. Essas amostras devem ser definidas primeiramente para as áreas de negócios e, em seguida, para os componentes de sistema em cada área de negócio selecionada. As amostras devem ser uma seleção representativa de todos os tipos e locais das áreas de negócios, bem como tipos de componentes de sistema nas áreas de negócio selecionadas. As amostras devem ser suficientemente amplas para fornecer ao assessor garantia de que os controles serão implementados conforme o esperado.

Exemplos de áreas de negócios incluem, entre outros, escritórios corporativos, lojas, locais de franquias, áreas de processamento, centros de dados e outros tipos de instalações em diferentes locais. Os exemplos devem incluir componentes de sistema em cada área de negócio. Por exemplo, para cada área de negócio, inclua uma série de sistemas operacionais, funções e aplicativos que são aplicáveis à área sob análise.

Como exemplo, o assessor pode definir uma amostra em uma área de negócios para incluir servidores Sun executando Apache, servidores Windows executando Oracle, sistemas do mainframe executando aplicativos de processamento de cartões herdados, servidores de transferência de dados executando HP-UX e servidores Linux executando MYSQL. Se todos os aplicativos forem executados a partir de um único SO (por exemplo, Windows 7 ou Solaris 10), então, o exemplo também deverá incluir vários aplicativos (por exemplo, servidores do banco de dados, servidores Web, servidores de transferência de dados).

Ao selecionar exemplos de áreas de negócios/componentes de sistema, os avaliadores devem considerar o seguinte:

- Se houver segurança, processos e controles operacionais do PCI DSS implementados de forma padrão e centralizada que garanta consistência e que cada área de negócio/componente de sistema deva seguir, a amostra poderá ser menor do que se não houver processos/controles padronizados implementados. A amostra deve ser ampla o bastante para fornecer ao assessor garantia razoável de que todas as áreas de negócio/componentes do sistema estejam configurados pelo processo padrão. O assessor deve verificar se os controles centralizados e padronizados estão implementados e funcionando de forma efetiva.
- Caso haja mais de um tipo de segurança e ou processo operacional padrão implementados (por exemplo, para tipos diferentes de áreas de negócio/componentes do sistema), a amostra deve ser ampla o bastante para incluir áreas de negócios/componentes do sistema seguros com cada tipo de processo.
- Caso não haja processos/controles padrão implementados e cada área de negócio/componente do sistema do PCI DSS seja gerenciado por meio de processos não padronizados, a amostra deve ser maior para o assessor se assegurar de que cada área de negócio/componente do sistema tenha implementado os requisitos do PCI DSS apropriadamente.

- As amostras de componentes do sistema devem incluir todos os tipos e combinações em uso. Por exemplo, quando os aplicativos servem como amostras, a amostra deve incluir todas as versões e plataformas para cada tipo de aplicativo.

Para cada instância em que a amostragem for usada, o assessor deverá:

- Registrar o argumento atrás da técnica de amostragem e do tamanho da amostragem,
- Registrar e validar os processos e controles padronizados do PCI DSS usados para determinar o tamanho da amostra e
- Explicar como a amostra é adequada e representativa da população geral.

**Consulte também:**

Apêndice D: Segmentação e amostragem de áreas de negócios/componentes do sistema.

Os avaliadores devem revalidar o argumento da amostragem para cada avaliação. Se a amostragem for utilizada, diferentes amostras de áreas de negócios e componentes do sistema devem ser selecionadas para cada avaliação.

## Controles de compensação

Anualmente, quaisquer controles de compensação devem ser documentados, revisados e validados pelo assessor e incluídos no envio do Relatório sobre conformidade, de acordo com o *Apêndice B: Controles de compensação* e *Apêndice C: Planilha dos controles de compensação*.

Para cada um dos controles de compensação, a Planilha dos controles de compensação (*Apêndice C*) **deve** ser preenchida. Além disso, os resultados dos controles de compensação devem ser registrados no ROC na seção de requisitos do PCI DSS correspondente.

Para obter mais detalhes sobre “controles de compensação”, consulte os *Apêndices B e C* mencionados acima.

## Instruções e conteúdo para o relatório sobre conformidade

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

O *Modelo de relatório ROC do PCI DSS* deve ser usado como modelo para gerar o *Relatório de conformidade*. A entidade avaliada deve seguir os requisitos de informe respectivos de cada bandeira de pagamento para assegurar que cada bandeira de pagamento reconheça o status de conformidade da entidade. Entre em contato com cada bandeira de pagamento ou adquirente para definir os requisitos e instruções de relatório.

## Processo de avaliação do PCI DSS

O processo de avaliação do PCI DSS inclui a conclusão das seguintes etapas:

1. Verifique o escopo da avaliação do PCI DSS.
2. Realize a avaliação do PCI DSS do ambiente, seguindo os procedimentos de teste para cada requisito.
3. Conclua o relatório aplicável para a avaliação [ou seja, o *Questionário de autoavaliação* (SAQ) ou Relatório de conformidade (ROC)], inclusive a documentação de todos os controles compensatórios, de acordo com as instruções e orientações aplicáveis do PCI.
4. Preencha por completo o atestado de conformidade referente aos prestadores de serviços ou comerciantes, conforme aplicável. Os atestados de conformidade estão disponíveis no site do PCI SSC.
5. Envie o SAQ ou ROC e o atestado de conformidade, junto com qualquer outra documentação solicitada, como relatórios de varredura de ASV, ao adquirente (para comerciantes) ou à bandeira de pagamento ou outro solicitante (para prestadores de serviços).
6. Se necessário, proceda à retificação para atender às exigências em descumprimento e forneça um relatório atualizado.

## Versões do PCI DSS

Na data de publicação deste documento, a v 3.1 do PCI DSS permanecerá em vigor até 31 de outubro de 2016, e prescreverá após o citado período. Todas as validações do PCI DSS após esta data deverão adotar a v 3.2 do PCI DSS ou versão posterior.

A tabela a seguir fornece um resumo das versões e datas de vigência do PCI DSS<sup>6</sup>.

Versão	Publicação:	Prescrição:
PCI DSS v3.2 (este documento)	Abril de 2016	A determinar
PCI DSS v3.1	Abril de 2015	31 de outubro de 2016

---

<sup>6</sup> Sujeitas a alterações após lançamento de uma nova versão do PCI DSS.

## Requisitos detalhados do PCI DSS e procedimentos da avaliação de segurança

As informações a seguir definem os cabeçalhos das colunas para os requisitos do PCI DSS e procedimentos da avaliação de segurança:

- **Requisitos do PCI DSS** – Esta coluna define os requisitos do padrão de segurança dos dados; a conformidade do PCI DSS é validada de acordo com esses requisitos.
- **Procedimentos de teste** – Esta coluna exibe os processos a serem seguidos pelo assessor para validar se os requisitos do PCI DSS têm sido atendidos e se estão “vigentes”.
- **Orientação** – Esta coluna descreve a intenção ou o objetivo de segurança por trás de cada um dos requisitos do PCI DSS. Esta coluna contém apenas orientação e tem o objetivo de auxiliar a compreender o porquê de cada requisito. A orientação nesta coluna não substitui ou expande os Requisitos do PCI DSS e Procedimentos de teste.

**Observação:** Os requisitos do PCI DSS não são considerados adequados se os controles ainda não estiverem implementados ou programados para estarem concluídos em uma data futura. Depois que qualquer item em aberto ou inadequado for reportado à entidade, o assessor fará uma reavaliação para validar se a solução 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 a conclusão de relatórios de conformidade (ROC), consulte o Modelo de relatório ROC do PCI DSS.
- Para obter instruções sobre a conclusão de questionários de autoavaliação (SAQ), consulte as Instruções e orientações SAQ do PCI DSS.
- Para obter instruções sobre o envio dos relatórios de validação de conformidade do PCI DSS, consulte os atestados de conformidade do PCI DSS.

## Construir e manter a segurança de rede e sistemas

### **Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão**

Firewalls são dispositivos do computador que controlam o tráfego do computador permitido entre a rede de uma empresa (interna) e redes não confiáveis (externa), assim como o tráfego dentro e fora de muitas áreas confidenciais na rede confiável interna de uma empresa. O ambiente de dados do titular do cartão é um exemplo de uma área mais sensível dentro da rede confiável de uma empresa.

Um firewall examina todo o tráfego da rede e bloqueia aquelas transmissões que não atendem aos critérios de segurança específicos.

Todos os sistemas devem ser protegidos do acesso não autorizado de redes não confiáveis, seja acessando o sistema por meio da internet como e-commerce, acesso à internet através dos navegadores na área de trabalho por parte dos funcionários, acesso via e-mail dos funcionários, conexão dedicada como conexões entre negócios, por meio de redes sem fio ou de outras fontes. Com frequência, trajetos aparentemente insignificantes que direcionam ou partem de redes não confiáveis podem fornecer caminhos não protegidos aos sistemas principais. Os firewalls são um mecanismo de proteção essencial para qualquer rede de computador.

Outros componentes do sistema podem oferecer a funcionalidade de firewall, contanto que atendam aos requisitos mínimos para firewalls, conforme definido no Requisito 1. Onde outros componentes do sistema forem usados no ambiente dos dados do titular do cartão para oferecer a funcionalidade do firewall, esses dispositivos deverão ser incluídos no escopo e na avaliação do Requisito 1.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
1.1 Defina e implemente os padrões de configuração do firewall e do roteador que incluam o seguinte:	1.1 Inspeccione os padrões de configuração do firewall e do roteador, além de outras documentações especificadas abaixo e verifique se os padrões estão concluídos e implementados conforme segue:	Firewalls e roteadores são os principais componentes da arquitetura que controlam a entrada e a saída da rede. Esses dispositivos são software ou hardware que bloqueiam acesso indesejado e gerenciam acesso autorizado de e para a rede.  Os procedimentos e padrões de configuração ajudarão a garantir que a primeira linha de defesa da organização na proteção de seus dados continue forte.
1.1.1 Um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador	1.1.1.a Examine os procedimentos documentados para saber se há um processo formal para testar e aprovar todas as: <ul style="list-style-type: none"> <li>• Conexões de rede e</li> <li>• Alterações nas configurações do roteador e do firewall</li> </ul>	Um processo documentado e implementado para aprovar e testar todas as conexões e alterações nos firewalls e roteadores ajudará a evitar problemas de segurança causados pela má configuração da rede, do roteador ou do firewall.  Sem a aprovação formal e teste das alterações, os registros das alterações podem não ser atualizados, o que pode levar à inconsistência entre a documentação de rede e a configuração em si.
	1.1.1.b Para obter uma amostra de conexões de rede, converse com o funcionário responsável e examine registros para verificar se elas foram aprovadas e testadas.	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>1.1.1.c</b> Identifique uma amostra de alterações reais realizadas nas configurações do roteador e do firewall, compare com os registros da alteração e converse com o funcionário responsável para verificar se as alterações foram aprovadas e testadas.</p>	
<p><b>1.1.2</b> Diagrama atual da rede que identifica todas as conexões entre o ambiente dos dados do titular do cartão e outras redes, incluindo qualquer rede sem fio</p>	<p><b>1.1.2.a</b> Analise o(s) diagrama(s) e observe as configurações de rede para saber se existe um diagrama de rede e se ele registra todas as conexões com relação aos dados do titular do cartão, incluindo quaisquer redes sem fio.</p> <p><b>1.1.2.b</b> Converse com o funcionário responsável para verificar se o diagrama é mantido atualizado.</p>	<p>Os diagramas de rede descrevem como as redes são configuradas e identificam a localização de todos os dispositivos de rede.</p> <p>Sem os diagramas da rede atual, os dispositivos podem ser ignorados e sem querer deixados de fora dos controles de segurança implementados para PCI DSS e, assim, vulneráveis ao comprometimento.</p>
<p><b>1.1.3</b> Diagrama atual que mostra todos os fluxos de dados do titular do cartão pelos sistemas e redes</p>	<p><b>1.1.3</b> Analise o diagrama do fluxo de dados e converse com o funcionário para verificar se o diagrama:</p> <ul style="list-style-type: none"> <li>• Mostra todos os fluxos de dados do titular do cartão pelos sistemas e redes.</li> <li>• É mantido atualizado conforme necessário em relação às alterações no ambiente.</li> </ul>	<p>Os diagramas de fluxo de dados do titular do cartão identificam a localização de todos os dados do titular do cartão que são armazenados, processados ou transmitidos dentro da rede.</p> <p>Os diagramas de fluxo de dados do titular do cartão e de rede ajudam uma organização a compreender e acompanhar o escopo de seu ambiente, mostrando como os dados do titular do cartão passam pelas redes e entre os dispositivos e sistemas individuais.</p>
<p><b>1.1.4</b> Requisitos para um firewall em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona de rede interna</p>	<p><b>1.1.4.a</b> Analise os padrões de configuração do firewall e verifique se eles incluem requisitos para um firewall em cada conexão da internet e entre qualquer DMZ e a zona de rede interna.</p> <p><b>1.1.4.b</b> Verifique se o diagrama da rede atual está de acordo com os padrões de configuração do firewall.</p> <p><b>1.1.4.c</b> Observe as configurações de rede para verificar se um firewall está implementado em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona de rede interna, conforme os padrões de configuração registrados e os diagramas de rede.</p>	<p>Usar um firewall em todas as conexões de internet que entram e saem da rede e entre qualquer DMZ e a rede interna permite que a organização monitore e controle o acesso e minimize as chances de um indivíduo mal-intencionado obter acesso à rede interna por meio de uma conexão não protegida.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>1.1.5</b> Descrição de grupos, funções e responsabilidades quanto ao gerenciamento dos componentes da rede</p>	<p><b>1.1.5.a</b> Verifique se os padrões de configuração do firewall e do roteador incluem uma descrição dos grupos, funções e responsabilidades quanto ao gerenciamento dos componentes da rede.</p>	<p>Essa descrição de funções e a atribuição das responsabilidades garante que os funcionários estejam cientes de quem é responsável pela segurança de todos os componentes da rede e que os responsáveis por gerenciar os componentes estejam cientes de suas responsabilidades. Se as funções e responsabilidades não forem atribuídas formalmente, os dispositivos podem ficar sem gerenciamento.</p>
	<p><b>1.1.5.b</b> Converse com o funcionário responsável pelo gerenciamento dos componentes da rede para confirmar se as funções e responsabilidades estão atribuídos conforme o que está registrado.</p>	
<p><b>1.1.6</b> Documentação de justificativa comercial e aprovação para uso de todos os serviços, protocolos e portas permitidas, inclusive documentação dos recursos de segurança implementados para os protocolos considerados não seguros.</p>	<p><b>1.1.6.a</b> Verifique se os padrões de configuração do firewall e roteador incluem uma lista documentada de todos os serviços, protocolos e portas, inclusive a justificativa e aprovação comercial para cada um.</p>	<p>Muitas vezes ocorrem comprometimentos decorrentes de portas e serviços não utilizados ou não seguros, visto que é frequente eles possuírem vulnerabilidades conhecidas e muitas organizações não aplicam patches nas vulnerabilidades para serviços, protocolos e portas que eles não utilizam (embora as vulnerabilidades ainda estejam presentes). Definindo e documentando claramente quais portas, serviços e portas são necessários para a empresa, as organizações podem garantir que todos os outros serviços, protocolos e portas sejam desabilitados ou removidos.</p> <p>As aprovações devem ser concedidas por pessoal independente da equipe de gerenciamento da configuração.</p> <p>Se portas, serviços e protocolos não seguros forem necessários para a empresa, o risco apresentado pelo uso desses protocolos deve ser claramente entendido e aceito pela organização, o uso do protocolo deve ser justificado e os recursos de segurança que permitem que esses protocolos sejam usados com segurança deverão ser documentados e implementados. Se esses serviços, portas e protocolos não seguros não forem necessários para a empresa, eles deverão ser desativados ou removidos.</p>
	<p><b>1.1.6.b</b> Identifique portas, serviços e protocolos não seguros permitidos e verifique se os recursos de segurança estão documentados para cada serviço.</p>	
	<p><b>1.1.6.c</b> Analise as configurações do roteador e do firewall para verificar se os recursos de segurança documentados estão implementados para cada porta, serviço e protocolo não seguros.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
		Para obter orientações sobre serviços, protocolos ou portas consideradas inseguras, consulte as instruções e normas para o setor (p. ex., NIST, ENISA, OWASP etc.).
<p><b>1.1.7</b> Requisito para analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses</p>	<p><b>1.1.7.a</b> Verifique se os padrões de configuração do firewall e do roteador exigem a análise dos conjuntos de regras do roteador e do firewall pelo menos a cada seis meses.</p> <p><b>1.1.7.b</b> Analise a documentação referente às revisões do conjunto de regras e converse com o funcionários para verificar se os conjuntos de regras são revisados pelo menos a cada seis meses.</p>	<p>Essa análise dá à organização a oportunidade de, pelo menos a cada seis meses, limpar todas as regras desnecessárias, obsoletas ou incorretas e garantir que todos os conjuntos de regras permitam apenas serviços e portas autorizados que correspondam às justificativas registradas de negócios.</p> <p>As organizações que possuem alto volume de alterações nos conjuntos de regras do roteador e do firewall podem querer realizar as revisões com mais frequência a fim de garantir que os conjuntos de regras continuem a atender as necessidades da empresa.</p>
<p><b>1.2</b> Elabore configurações de firewall e roteador que restrinjam as conexões entre redes não confiáveis e quaisquer componentes do sistema no ambiente de dados do titular do cartão.</p> <p><b>Observação:</b> Uma “rede não confiável” é qualquer rede que seja externa às redes que pertencem à entidade em análise e/ou que esteja além da capacidade da entidade de controlar ou gerenciar.</p>	<p><b>1.2</b> Examine as configurações do firewall e do roteador para verificar se as conexões estão restritas entre as redes não confiáveis e os componentes de sistema no ambiente de dados do titular do cartão:</p>	<p>É essencial instalar proteção de rede entre a rede interna e confiável e qualquer rede não confiável que seja externa e/ou fique fora da capacidade de controle ou gerenciamento da entidade. A falha em implementar essa medida de forma correta resulta na vulnerabilidade da entidade ao acesso não autorizado de indivíduos ou softwares mal-intencionados.</p> <p>Para que a funcionalidade do firewall seja eficaz, ele deve ser configurado corretamente para controlar e/ou limitar o tráfego dentro e fora da rede da entidade.</p>
<p><b>1.2.1</b> Restrinja o tráfego de entrada e saída ao que é necessário ao ambiente de dados do titular do cartão e rejeite especificadamente todos os outros tráfegos.</p>	<p><b>1.2.1.a</b> Analise os padrões de configuração do roteador e do firewall para verificar se eles identificam o tráfego de entrada e saída necessário para o ambiente de dados do titular do cartão.</p> <p><b>1.2.1.b</b> Analise as configurações do roteador e do firewall para verificar se o tráfego de entrada e saída está limitado ao que é necessário para o ambiente de dados do titular do cartão.</p>	<p>A análise de todas as conexões de entrada e saída permite a inspeção e restrição de tráfego com base na fonte e/ou endereço de destino, evitando assim o acesso não filtrado entre ambientes confiáveis e não confiáveis. Isso evita que indivíduos mal intencionados acessem a rede da entidade por meio de endereços IP não autorizados ou usem serviços, protocolos ou portas de forma não autorizada (por exemplo,</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>1.2.1.c</b> Analise as configurações do roteador e do firewall para verificar se todos os outros tráfegos de entrada e saída são recusados de forma específica, por exemplo, ao usar a opção explícita “recusar todos” ou uma recusa implícita após a declaração de permissão.</p>	<p>enviar dados obtidos dentro da rede da entidade para um servidor não confiável).</p> <p>Implementar uma regra que rejeite todos os tráfegos de entrada e saída não necessários ajuda a evitar violações acidentais que permitam que tráfego potencialmente prejudicial entre ou saia.</p>
<p><b>1.2.2</b> Proteja e sincronize os arquivos de configuração do roteador.</p>	<p><b>1.2.2.a</b> Analise os arquivos de configuração do roteador para verificar se eles estão seguros em relação ao acesso não autorizado.</p> <p><b>1.2.2.b</b> Analise as configurações do roteador para verificar se eles estão sincronizados, por exemplo, a configuração executada (ou ativa) corresponde à configuração de inicialização (usada quando as máquinas são ligadas).</p>	<p>Enquanto os arquivos de configuração do roteador executados (ou ativos) incluem as configurações seguras e atuais, os arquivos de inicialização (que são usados quando os roteadores são reiniciados ou ligados) devem ser atualizados com as mesmas configurações seguras para garantir que estas configurações sejam aplicadas quando a configuração de inicialização é executada.</p> <p>Por serem executados apenas de vez em quando, os arquivos de configuração de inicialização são frequentemente esquecidos e não são atualizados. Quando o roteador reinicializar e carregar uma configuração de inicialização que não tenha sido atualizada com as mesmas configurações seguras que a configuração de execução, isso pode resultar em regras mais fracas que permitam que indivíduos mal-intencionados entrem na rede.</p>
<p><b>1.2.3</b> Instale firewalls de perímetro entre todas as redes sem fio e o ambiente de dados do titular do cartão e configure esses firewalls para recusar ou, se o tráfego for necessário para fins comerciais, permitir apenas tráfego autorizado entre o ambiente sem fio e o ambiente de dados do titular do cartão.</p>	<p><b>1.2.3.a</b> Analise as configurações do firewall e do roteador para verificar se há firewalls de perímetro instalados entre todas as redes sem fio e o ambiente de dados do titular do cartão.</p> <p><b>1.2.3.b</b> Verifique se os firewalls recusam ou, se o tráfego for necessário para fins comerciais, permitem apenas tráfego autorizado entre o ambiente sem fio e o ambiente de dados do titular do cartão.</p>	<p>A implementação conhecida (ou desconhecida) e a exploração da tecnologia sem fio dentro de uma rede é um caminho comum para indivíduos mal-intencionados ganharem acesso à rede e aos dados do titular do cartão. Se um dispositivo sem fio ou uma rede forem instalados sem o conhecimento da entidade, um indivíduo mal-intencionado pode fácil e “invisivelmente” entrar na rede. Se os firewalls não restringirem o acesso das redes sem fio no CDE, indivíduos mal-intencionados que tiverem acesso não autorizado à rede sem fio poderão se conectar facilmente ao</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
		<p>CDE e comprometer as informações da conta.</p> <p>Deverão ser instalados firewalls entre todas as redes sem fio e o CDE, independentemente da finalidade do ambiente com o qual a rede sem fio estiver conectada. Isto pode incluir, entre outros, redes corporativas, revendedores, redes de acesso ao visitante, ambientes de armazenamento, etc.</p>
<p><b>1.3</b> Proíba o acesso público direto entre a internet e qualquer componente do sistema no ambiente de dados do titular do cartão.</p>	<p><b>1.3</b> Analise as configurações do firewall e do roteador (incluindo, entre outros, roteador de suspensão na internet, o roteador DMZ e o firewall, o segmento DMZ do titular do cartão, o roteador de perímetro e o segmento interno da rede do titular do cartão) e realizar o que segue para determinar que não haja acesso direto entre a internet e os componentes do sistema no segmento interno da rede de dados do titular do cartão:</p>	<p>Embora possa haver razões legítimas para conexões não confiáveis a serem autorizadas nos sistemas da DMZ (por exemplo, permitir acesso do público a um servidor da web), tais conexões jamais devem ser concedidas aos sistemas na rede interna. O objetivo de um firewall é gerenciar e controlar todas as conexões entre os sistemas públicos e internos, especialmente aqueles que armazenam, processam ou transmitem os dados do titular do cartão. Se for permitido o acesso direto entre sistemas públicos e o CDE, as proteções oferecidas pelo firewall serão ignoradas e os componentes do sistema que armazenam os dados do titular do cartão poderão ser comprometidos.</p>
<p><b>1.3.1</b> Implemente uma DMZ para limitar o tráfego somente para componentes do sistema que oferece serviços, protocolos e portas acessíveis publicamente.</p>	<p><b>1.3.1</b> Analise as configurações do firewall e do roteador para verificar se uma DMZ foi implementada para limitar o tráfego somente para componentes do sistema que ofereça serviços, protocolos e portas acessíveis publicamente.</p>	<p>O DMZ é a parte da rede responsável pelo gerenciamento das conexões entre a internet (ou redes não confiáveis) e os serviços que uma empresa precisa disponibilizar para o público (como um servidor Web).</p>
<p><b>1.3.2</b> Limite o tráfego de entrada da internet a endereços IP na DMZ.</p>	<p><b>1.3.2</b> Analise as configurações do firewall e do roteador para verificar se o tráfego de entrada da internet está limitado a endereços IP na DMZ.</p>	<p>Este recurso será utilizado para evitar que indivíduos mal-intencionados acessem a rede interna da empresa pela internet ou por meio de serviços, protocolos ou portas de forma não autorizada.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>1.3.3</b> Implemente medidas contra falsificação para detectar e impedir que endereços IP de fonte falsificada entrem na rede.</p> <p>(Por exemplo, bloquear tráfego originado da internet com um endereço de fonte interna).</p>	<p><b>1.3.3</b> Analise as configurações do firewall e do roteador para verificar se as medidas contra falsificação estão implementadas, por exemplo, os endereços internos não conseguem passar da internet para a DMZ.</p>	<p>Normalmente, um pacote contém o endereço IP do computador que originalmente o enviou para que os outros computadores da rede saibam de onde vem o pacote. Indivíduos mal-intencionados tentarão falsificar (ou copiar) o endereço de envio do IP para que o sistema alvo acredite que o pacote seja de uma fonte confiável.</p> <p>Filtrar pacotes que entram na rede ajuda, entre outras coisas, a garantir que os pacotes não sofram falsificação, parecendo que vêm da própria rede interna da organização.</p>
<p><b>1.3.4</b> Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a internet.</p>	<p><b>1.3.4</b> Analise as configurações do firewall e do roteador para verificar se o tráfego de saída do ambiente de dados do titular do cartão para a internet está explicitamente autorizado.</p>	<p>Todo o tráfego que sair do ambiente de dados do titular do cartão deverá ser avaliado para garantir que esteja de acordo com as regras autorizadas preestabelecidas. As conexões deverão ser inspecionadas para restringir o tráfego de forma a permitir apenas as comunicações autorizadas (por exemplo restringindo portas/endereços de origem/destino ou bloqueando o conteúdo).</p>
<p><b>1.3.5</b> Somente autorize conexões “estabelecidas” na rede.</p>	<p><b>1.3.5</b> Examine as configurações do firewall e do roteador para verificar se o firewall permite somente conexões estabelecidas na rede interna e impede conexões de entrada não associadas a uma sessão anteriormente estabelecida.</p>	<p>Um firewall que mantém o “status” (ou estado) para cada conexão estabelecida através do firewall sabe se uma resposta aparente para uma conexão anterior é realmente válida e autorizada (já que preserva cada status de conexão) ou se é tráfego mal intencionado tentando enganar o firewall para que a conexão seja permitida.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>1.3.6</b> Implemente os componentes do sistema que armazenam dados do titular do cartão (como banco de dados) em uma zona da rede interna separada da DMZ e de outras redes não confiáveis.</p>	<p><b>1.3.6</b> Analise as configurações do firewall e do roteador para verificar se os componentes do sistema que armazenam dados do titular do cartão estão em uma zona da rede interna separada da DMZ e de outras redes não confiáveis.</p>	<p>Se os dados do titular do cartão estiverem localizados dentro da DMZ, o acesso a essas informações será mais fácil para um invasor externo, pois há poucas camadas a serem penetradas. Proteger os componentes do sistema que armazenam os dados do titular do cartão em uma zona de rede interna separada da DMZ e de outras redes não confiáveis com um firewall pode evitar que um tráfego de rede não autorizado alcance o componente do sistema.</p> <p><b>Observação:</b> Este requisito não se aplica ao armazenamento temporário dos dados do titular do cartão em memória volátil.</p>
<p><b>1.3.7</b> Não divulgue endereços IP privados e informações de roteamento a partes não autorizadas.</p> <p><b>Observação:</b> os métodos para ocultar o endereço IP podem incluir, entre outros:</p> <ul style="list-style-type: none"> <li>• Conversão de endereços de rede (NAT)</li> <li>• Implementação dos servidores contendo dados do titular do cartão atrás dos servidores de proxy/firewalls</li> <li>• Remoção ou filtragem das propagandas de rota para redes privadas que empregam endereçamento registrado</li> <li>• Uso interno do espaço de endereço RFC1918 em vez de endereço registrado.</li> </ul>	<p><b>1.3.7.a</b> Analise as configurações do firewall e do roteador para verificar se os métodos estão implementados para evitar a divulgação de endereços IP privados e informações de roteamento das redes internas para a internet.</p> <p><b>1.3.7.b</b> Converse com os funcionários e analise a documentação para verificar se qualquer divulgação de endereços IP privados e informações de roteamento para entidades externas está autorizada.</p>	<p>Restringir a divulgação de endereços IP internos ou privados é essencial para evitar que os hackers “descubram” os endereços IP da rede interna e utilizem essas informações para acessar a rede.</p> <p>Os métodos usados para atender à intenção deste requisito podem variar de acordo com a tecnologia de rede específica utilizada. Por exemplo, os controles utilizados para atender a estes requisitos em redes IPv4 poderão ser diferentes daqueles utilizados em redes IPv6.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>1.4</b> Instale um software de firewall pessoal ou função equivalente em qualquer dispositivo portátil (inclusive de propriedade da empresa e/ou do funcionário) que se conecte à internet quando fora da rede (por exemplo, laptops usados pelos funcionários) e que também seja usado para acessar o CDE. As configurações do firewall (ou equivalente) incluem:</p> <ul style="list-style-type: none"> <li>Os ajustes específicos de configuração são definidos.</li> <li>O firewall pessoal (ou função equivalente) é executado ativamente.</li> <li>O firewall pessoal (ou função equivalente) não pode ser alterado pelos usuários dos dispositivos de computação portáteis.</li> </ul>	<p><b>1.4.a</b> Analise as políticas e padrões de configuração para verificar:</p> <ul style="list-style-type: none"> <li>Um software de firewall pessoal ou função equivalente é requerido para todos os dispositivos portáteis (inclusive de propriedade da empresa e/ou do funcionário) que se conectem à internet quando fora da rede (por exemplo, laptops usados pelos funcionários) e que também sejam usados para acessar o CDE.</li> <li>Ajustes específicos de configuração são definidos para o firewall pessoal (ou função equivalente).</li> <li>O firewall pessoal (ou função equivalente) é configurado para execução ativa.</li> <li>O firewall pessoal (ou função equivalente) é configurado para não ser alterado pelos usuários dos dispositivos de computação portáteis.</li> </ul> <p><b>1.4.b</b> Inspeccione uma amostra dos dispositivos pertencentes à empresa e/ou ao funcionário para verificar se:</p> <ul style="list-style-type: none"> <li>O firewall pessoal (ou função equivalente) está instalado e configurado conforme os ajustes de configuração específicos da organização.</li> <li>O firewall pessoal (ou função equivalente) é executado ativamente.</li> <li>O firewall pessoal (ou função equivalente) não pode ser alterado pelos usuários dos dispositivos de computação portáteis.</li> </ul>	<p>Os dispositivos portáteis de computação que têm permissão para conectar-se à internet fora do firewall corporativo são mais vulneráveis às ameaças baseadas na internet. O uso da função firewall (p. ex., software ou hardware de firewall pessoal) ajuda a proteger os dispositivos de invasões via internet, que poderiam usar o dispositivo para obter acesso aos dados e sistemas da organização, uma vez que o dispositivo é reconectado à rede.</p> <p>Os ajustes específicos das configurações do firewall são determinados pela organização.</p> <p><b>Observação:</b> Este requisito aplica-se a dispositivos de computação pertencentes ao funcionário e à empresa. Os sistemas que não podem ser gerenciados pelas políticas corporativas introduzem fraquezas e fornecem oportunidades que podem ser exploradas por pessoas mal intencionadas. Permitir que sistemas não confiáveis conectem-se ao CDE da organização pode resultar em acesso concedido a invasores e outros usuários mal intencionados.</p>
<p><b>1.5</b> Certifique-se de que as políticas de segurança e procedimentos operacionais do gerenciamento dos firewalls estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>1.5</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e procedimentos operacionais do gerenciamento dos firewalls estão:</p> <ul style="list-style-type: none"> <li>Documentados,</li> <li>Em uso, e</li> <li>Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para garantir que os firewalls e roteadores sejam continuamente gerenciados a fim de evitar o acesso não autorizado à rede.</p>

**Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança**

Indivíduos mal-intencionados (dentro e fora de uma empresa) com frequência usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bastante conhecidas pelas comunidades de hackers e facilmente determinadas por meio de informações públicas.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.1</b> Sempre altere os padrões disponibilizados pelo fornecedor e remova ou desabilite contas padrão desnecessárias <b>antes de</b> instalar um sistema na rede.</p> <p>Isso se aplica a TODAS as senhas padrão, inclusive, entre outras, às utilizadas pelos sistemas operacionais, softwares que fornecem serviços de segurança, aplicativos e contas do sistema, terminais de ponto de venda (POS), solicitações de pagamento, strings de comunidade do Protocolo de Gerenciamento de Rede Simples (SNMP), etc.</p>	<p><b>2.1.a</b> Escolha uma amostra dos componentes do sistema e tente acessar (com a ajuda do administrador do sistema) os dispositivos e aplicativos usando as contas e senhas padrão disponibilizadas pelo fornecedor, para verificar se TODAS as senhas padrão (incluindo as que estão nos sistemas operacionais, software que oferece serviços de segurança, aplicativos e contas de sistema, terminais POS e strings de comunidade SNMP (Simple Network Management Protocol)) foram alteradas. (Use os manuais do fornecedor e as fontes na internet para localizar as contas/senhas disponibilizadas pelo fornecedor.)</p> <p><b>2.1.b</b> Para obter um exemplo dos componentes do sistema, verifique se todas as contas padrão desnecessárias (incluindo contas usadas pelos sistemas operacionais, software de segurança, aplicativos, sistemas, terminais POS, SNMP, etc.) foram removidas ou desabilitadas.</p> <p><b>2.1.c</b> Converse com os funcionários e analise a documentação de suporte para verificar se:</p> <ul style="list-style-type: none"> <li>• Todas as senhas padrão (incluindo senhas padrão em sistemas operacionais, software que oferece serviços de segurança, aplicativos e contas do sistema, terminais POS, strings de comunidade SNMP (Simple Network Management Protocol), etc.) são alteradas antes de um sistema ser instalado na rede.</li> <li>• Contas padrão desnecessárias (incluindo contas usadas pelos sistemas operacionais, software de segurança, aplicativos, sistemas, terminais POS, SNMP, etc.) são removidas ou desabilitadas antes de um sistema ser instalado na rede.</li> </ul>	<p>Indivíduos mal-intencionados (dentro e fora de uma empresa) com frequência usam as configurações, nomes de conta e senhas padrão do fornecedor para comprometer o software do sistema operacional, aplicativos e os sistemas nos quais eles estão instalados. Por estas configurações padrão serem frequentemente publicadas e bem conhecidas nas comunidades de hackers, alterar estas configurações deixará os sistemas menos vulneráveis a invasões.</p> <p>Mesmo se uma conta padrão não tem o objetivo de ser usada, alterar a senha padrão para uma senha forte e exclusiva e então desabilitar a conta evitará que um indivíduo mal-intencionado reabilite a conta e obtenha acesso com a senha padrão.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.1.1</b> Em ambientes sem fio conectados ao ambiente de dados do titular do cartão ou que transmitam dados do titular do cartão, altere TODOS os padrões sem fio do fornecedor na instalação, inclusive, entre outros, chaves de criptografia padrão sem fio, senhas e strings de comunidades do SNMP.</p>	<p><b>2.1.1.a</b> Converse com os funcionários responsáveis e analise a documentação de suporte para verificar se:</p> <ul style="list-style-type: none"> <li>• As chaves de criptografia foram modificadas a partir do padrão na instalação</li> <li>• As chaves de criptografia padrão são modificadas sempre que um funcionário que conhece as chaves sai da empresa ou troca de cargo.</li> </ul>	<p>Se as redes sem fio não forem implementadas com configurações de segurança suficientes (incluindo a alteração das configurações padrão), os sniffers da rede sem fio conseguem espreitar o tráfego, capturar dados e senhas e entrar e invadir a sua rede com facilidade.</p> <p>Além disso, o protocolo de troca de chaves para versões mais antigas da criptografia 802.11x (Wired Equivalent Privacy ou WEP) foi quebrado e pode tornar a criptografia inútil. O firmware dos dispositivos deve estar atualizado para suportar protocolos mais seguros.</p>
	<p><b>2.1.1.b</b> Converse com os funcionários e consulte a as políticas e procedimentos para verificar se:</p> <ul style="list-style-type: none"> <li>• As strings de comunidades de SNMP padrão precisam ser modificadas na instalação.</li> <li>• As senhas/frases de senha padrão nos pontos de acesso devem ser alteradas na instalação.</li> </ul>	
	<p><b>2.1.1.c</b> Consulte a documentação do fornecedor e conecte-se aos dispositivos sem fio, com a ajuda do administrador do sistema, para verificar se:</p> <ul style="list-style-type: none"> <li>• As strings de comunidades de SNMP padrão não são utilizadas.</li> <li>• As senhas padrão dos pontos de acesso não são utilizadas.</li> </ul>	
	<p><b>2.1.1.d</b> Consulte a documentação do fornecedor e observe os ajustes da configuração sem fio para verificar se o firmware nos dispositivos sem fio foi atualizado para ser compatível com a criptografia forte para:</p> <ul style="list-style-type: none"> <li>• Autenticação em redes sem fio</li> <li>• Transmissão em redes sem fio.</li> </ul>	
	<p><b>2.1.1.e</b> Analise a documentação do fornecedor e observe os ajustes da configuração sem fio para verificar se outros padrões sem fio do fornecedor ligados à segurança foram alterados, se aplicável.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.2</b> Desenvolva padrões de configuração para todos os componentes do sistema. Certifique-se de que esses padrões abrangem todas as vulnerabilidades de segurança conhecidas e estão em conformidade com os padrões de fortalecimento do sistema aceitos pelo setor.</p> <p>As fontes dos padrões de proteção do sistema aceitos pelo setor podem incluir, entre outros:</p> <ul style="list-style-type: none"> <li>• Center for Internet Security (CIS)</li> <li>• International Organization for Standardization (ISO)</li> <li>• Instituto SysAdmin Audit Network Security (SANS)</li> <li>• National Institute of Standards and Technology (NIST).</li> </ul>	<p><b>2.2.a</b> Analise os padrões de configuração do sistema da organização para todos os tipos de componentes do sistema e verifique se os padrões de configuração do sistema são consistentes com os padrões de proteção aceitos pelo setor.</p> <p><b>2.2.b</b> Analise as políticas e questione os funcionários para verificar se os padrões de configuração do sistema estão atualizados conforme novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.1.</p> <p><b>2.2.c</b> Analise as políticas e questione os funcionários para verificar se os padrões de configuração do sistema são aplicados quando novos sistemas são configurados e considerados adequados antes de o sistema ser instalado na rede.</p> <p><b>2.2.d</b> Verifique se os padrões de configuração do sistema incluem os seguintes procedimentos para todos os tipos de componentes do sistema:</p> <ul style="list-style-type: none"> <li>• Alteração de todos os padrões informados pelo fornecedor e eliminação de contas padrão desnecessárias</li> <li>• Implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor</li> <li>• Habilitar apenas serviços, protocolos, daemons, etc. necessários, conforme exigido para a função do sistema</li> <li>• Implantar recursos de segurança adicionais para todos os serviços, protocolos ou daemons exigidos que forem considerados não seguros</li> <li>• Configurar os parâmetros de segurança do sistema para impedir o uso incorreto</li> <li>• Remover todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários.</li> </ul>	<p>Existem pontos fracos conhecidos em vários sistemas operacionais, bancos de dados e aplicativos empresariais, além disso existem também formas conhecidas de configurar esses sistemas para corrigir as vulnerabilidades de segurança. Para ajudar quem não é especialista em segurança, as organizações de segurança criaram recomendações e orientações para proteção do sistema que aconselham como corrigir esses pontos fracos.</p> <p>Exemplos de fontes para orientação sobre padrões de configuração incluem, entre outros: <a href="http://www.nist.gov">www.nist.gov</a>, <a href="http://www.sans.org">www.sans.org</a>, <a href="http://www.cisecurity.org">www.cisecurity.org</a>, <a href="http://www.iso.org">www.iso.org</a> e fornecedores do produto.</p> <p>Os padrões de configuração do sistema deverão ser mantidos atualizados para garantir que as deficiências recentemente identificadas sejam corrigidas antes de o sistema ser instalado na rede.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.2.1</b> Implemente somente uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor. (Por exemplo, servidores Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.)</p> <p><b>Observação:</b> Onde tecnologias de virtualização estiverem em uso, implemente somente uma função principal por componente do sistema virtual.</p>	<p><b>2.2.1.a</b> Selecione uma amostra dos componentes do sistema e inspecione as configurações do sistema para verificar se somente uma função principal está implementada por servidor.</p> <p><b>2.2.1.b</b> Se forem usadas tecnologias de virtualização, inspecione as configurações do sistema para verificar se somente uma função principal está implementada por componente ou dispositivo do sistema virtual.</p>	<p>Se funções do servidor que precisam de diferentes níveis de segurança estiverem localizadas no mesmo servidor, o nível de segurança das funções com maior necessidade de segurança pode ser reduzido devido à presença das funções de menor segurança. Além disso, as funções do servidor com menor nível de segurança podem apresentar falhas da segurança para outras funções no mesmo servidor. Considerando as necessidades de segurança de diferentes funções do servidor como parte dos padrões de configuração do sistema e processos relacionados, as organizações podem garantir que as funções que exigem diferentes níveis de segurança não coexistam no mesmo servidor.</p>
<p><b>2.2.2</b> Habilite somente serviços, protocolos, daemons, etc., necessários para a função do sistema.</p>	<p><b>2.2.2.a</b> Selecione uma amostra dos componentes do sistema e inspecione os serviços, daemons e protocolos do sistema ativado para verificar se apenas os serviços ou protocolos necessários estão habilitados.</p> <p><b>2.2.2.b</b> Identifique qualquer serviço, daemons ou protocolos não seguros que estejam habilitados e questione os funcionários para verificar se eles têm justificativa conforme os padrões de configuração documentados.</p>	<p>Conforme informado no item 1.1.6, existem muitos protocolos de que uma empresa pode precisar (ou estarem ativados por padrão) que normalmente são usados por indivíduos mal-intencionados para comprometer uma rede. Incluir este requisito como parte dos padrões de configuração da empresa e dos processos relacionados garante que apenas os serviços e protocolos necessários sejam habilitados.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.2.3</b> Implemente recursos de segurança adicionais para todos os serviços, protocolos ou daemons exigidos considerados não seguros.</p> <p><b>Observação:</b> Onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.</p>	<p><b>2.2.3.a</b> Inspeção os ajustes de configuração para verificar se os recursos de segurança estão documentados e implementados para todos os serviços, daemons ou protocolos.</p> <p><b>2.2.3.b</b> Se o SSL/TSL antigo estiver em uso, executar os procedimentos de teste previstos no Apêndice A2: <i>Requisitos adicionais do PCI DSS para entidades que usam SSL/TLS antigo.</i></p>	<p>Habilitar recursos de segurança antes que novos servidores sejam implantados evitará que os servidores sejam instalados no ambiente com configurações não seguras.</p> <p>Garantir que todos os serviços, protocolos e daemons não seguros estejam adequadamente protegidos com recursos de segurança apropriados dificulta que indivíduos mal-intencionados se aproveitem dos pontos de comprometimento normalmente usados dentro de uma rede.</p> <p>Consultar os padrões e as práticas recomendadas para o setor para obter informações sobre criptografia robusta e protocolos seguros (p. ex., NIST SP 800-52 e SP 800-57, OWASP etc.).</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.2.4</b> Configure os parâmetros de segurança do sistema para impedir o uso incorreto.</p>	<p><b>2.2.4.a</b> Converse com os administradores do sistema e/ou os gerentes de segurança para verificar se eles conhecem as configurações comuns dos parâmetros de segurança referentes aos componentes do sistema.</p> <p><b>2.2.4.b</b> Analise os padrões de configuração do sistema para verificar se as configurações comuns dos parâmetros de segurança estão incluídas.</p> <p><b>2.2.4.c</b> Selecione uma amostra dos componentes do sistema e inspecione os parâmetros comuns de segurança para verificar se eles estão ajustados corretamente e de acordo com os padrões de configuração.</p>	<p>Os padrões de configuração do sistema de sua organização e os processos relacionados devem abordar especificamente as configurações e os parâmetros de segurança que tenham implicações de segurança conhecidas para cada tipo de sistema em uso.</p> <p>Para que os sistemas sejam configurados corretamente, os funcionários responsáveis pela configuração e/ou administração dos sistemas devem ter conhecimento dos parâmetros específicos de segurança e ajustes que se aplicam ao sistema.</p>
<p><b>2.2.5</b> Remova todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários.</p>	<p><b>2.2.5.a</b> Selecione uma amostra dos componentes do sistema e inspecione as configurações para verificar se todas as funcionalidades desnecessárias (por exemplo, scripts, drivers, recursos, subsistemas, sistemas de arquivo, etc.) foram removidas.</p> <p><b>2.2.5.b.</b> Consulte a documentação e os parâmetros de segurança para verificar se as funções ativadas estão documentadas e suportam a configuração segura.</p> <p><b>2.2.5.c.</b> Consulte a documentação e os parâmetros de segurança para verificar se somente as funcionalidades registradas estão presentes nos componentes do sistema da amostra.</p>	<p>Funções desnecessárias podem gerar oportunidades adicionais para indivíduos mal-intencionados obterem acesso ao sistema. Removendo funcionalidades desnecessárias, as organizações podem se concentrar em proteger as funções exigidas e reduzir o risco de funções desconhecidas serem aproveitadas.</p> <p>Incluir isto nos padrões de proteção do servidor e processos resolve as implicações de segurança específicas associadas a funções desnecessárias (por exemplo, removendo/desativando FTP ou o servidor Web, caso o servidor não execute essas funções).</p>
<p><b>2.3</b> Criptografe todo o acesso administrativo que não utiliza console durante a criptografia forte.</p> <p><b>Observação:</b> Onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.</p>	<p><b>2.3</b> Selecione uma amostra dos componentes do sistema e verifique se o acesso administrativo que não utiliza console é criptografado realizando o que segue:</p> <p><b>2.3.a</b> Observe um administrador efetuar logon em cada sistema e analise as configurações do sistema para verificar se o método de criptografia forte é invocado antes da senha do administrador ser solicitada.</p> <p><b>2.3.b</b> Analise os serviços e os arquivos de parâmetro nos sistemas para determinar se o Telnet e outros comandos de logon remoto não seguros não estão disponíveis para o</p>	<p>Se a administração que não utiliza console (incluindo remota) não usa autenticação segura e comunicações criptografadas, informações confidenciais de nível administrativo ou operacional (como as senhas e IDs do administrador) poderão ser reveladas a um espião. Um indivíduo mal-intencionado pode usar essas informações para acessar a rede, tornar-se administrador e roubar os dados.</p> <p>Protocolos de texto simples (como HTTP, telnet, etc.) não criptografam detalhes de tráfego ou acesso, facilitando que um espião intercepte estas</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	acesso que não utiliza console.	informações.
	<p><b>2.3.c</b> Observe um administrador efetuar logon em cada sistema para verificar se o acesso do administrador às interfaces de gerenciamento baseadas na Web é criptografado com criptografia forte.</p> <p><b>2.3.d</b> Analise a documentação do fornecedor e questione os funcionários para verificar se a criptografia forte para a tecnologia utilizada está implementada de acordo com as práticas recomendadas do setor e/ou recomendações do fornecedor.</p> <p><b>2.3.e</b> Se o SSL/TLS antigo estiver em uso, executar os procedimentos de teste previstos no <i>Apêndice A2: Requisitos adicionais do PCI DSS para entidades que usam SSL/TLS antigo</i>.</p>	<p>Para serem considerados com “criptografia robusta”, os protocolos reconhecidos pelo setor com resistências de chave adequadas e gerenciamento de chave devem estar corretos conforme aplicável para o tipo de tecnologia utilizada. (Consultar “criptografia robusta” no Glossário de termos, abreviaturas e acrônimos do <i>PCI DSS</i> e do <i>PA-DSS</i>, e segundo os padrões e práticas recomendadas pelo setor, como NIST SP 800-52 e SP 800-57, OWASP etc.)</p>
<p><b>2.4</b> Mantenha uma relação dos componentes do sistema que estão no escopo do PCI DSS.</p>	<p><b>2.4.a</b> Analise a relação do sistema para verificar se uma lista de componentes de hardware e software é mantida e se inclui uma descrição da função/uso de cada um deles.</p> <p><b>2.4.b</b> Converse com os funcionários para verificar se uma relação documentada é mantida no momento.</p>	<p>Manter uma lista atual de todos os componentes do sistema permite que a organização defina de forma precisa e eficaz o escopo de seu ambiente para implementar os controles do PCI DSS. Sem uma relação, alguns componentes do sistema podem ser esquecidos e excluídos sem querer dos padrões de configuração da organização.</p>
<p><b>2.5</b> Certifique-se de que as políticas de segurança e procedimentos operacionais do gerenciamento dos padrões do fornecedor e outros parâmetros de segurança estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>2.5</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e procedimentos operacionais do gerenciamento dos padrões do fornecedor e outros parâmetros de segurança estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais diários para garantir que os padrões do fornecedor e outros parâmetros de segurança sejam continuamente gerenciados a fim de evitar configurações não seguras.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>2.6</b> Os provedores de hospedagem compartilhada devem proteger cada ambiente hospedado da entidade e os dados do titular do cartão. Esses provedores devem atender a requisitos específicos, conforme detalhado no <i>Apêndice A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada</i>.</p>	<p><b>2.6</b> Executar os procedimentos de teste <b>A.1.1</b> via <b>A.1.4</b>, conforme detalhados no <i>Apêndice A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada</i> para avaliações do PCI DSS dos provedores de hospedagem compartilhada para verificar se os provedores de hospedagem compartilhada protegem o ambiente hospedado e os dados das suas entidades (comerciantes e prestadores de serviços).</p>	<p>Isso serve para provedores de hospedagem que oferecem ambientes de hospedagem compartilhada para vários clientes no mesmo servidor. Quando todos os dados estiverem no mesmo servidor e sob o controle de um único ambiente, as configurações nestes servidores compartilhados frequentemente não são gerenciáveis pelos clientes individuais. Isto permite que os clientes adicionem funções e scripts não seguros que causam impacto na segurança de todos os outros ambientes de clientes e, assim, facilitando para um indivíduo mal-intencionado comprometer os dados de um cliente, obtendo acesso a todos os dados dos outros clientes. Consulte o <i>Apêndice A1</i> para verificar detalhes referentes aos requisitos.</p>

## Proteger os dados do titular do cartão

### Requisito 3: Proteger os dados armazenados do titular do cartão

Métodos de proteção como criptografia, truncamento, mascaramento e codificação Hash são componentes essenciais para proteção de dados do titular do cartão. Se um invasor burlar outros controles de segurança e obtiver acesso aos dados criptografados, sem as chaves criptográficas adequadas, os dados estarão ilegíveis e inutilizáveis para aquele indivíduo. Outros métodos eficientes de proteção dos dados armazenados também devem ser considerados como oportunidades potenciais de minimização dos riscos. Por exemplo, os métodos para minimizar riscos incluem não armazenar dados do titular do cartão, a menos que seja absolutamente necessário, truncar dados do titular do cartão se o PAN completo não for necessário e não enviar PAN usando tecnologias de mensagens ao usuário final, como e-mails e mensagens instantâneas.

Consulte a seção *Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS* para obter definições de “criptografia forte” e outros termos do PCI DSS.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.1</b> Mantenha a armazenagem dos dados do titular do cartão o mínimo possível, implementando políticas, processos e procedimentos de retenção e descarte de dados que incluem, pelo menos, o que segue para todo o armazenamento de dados do titular do cartão (CHD):</p> <ul style="list-style-type: none"> <li>• Limitar a quantia de dados armazenados e o tempo de retenção às restrições conforme exigências legais, regulatórias e/ou comerciais</li> <li>• Requisitos de retenção específicos para dados do titular do cartão</li> <li>• Processos para exclusão segura de dados quando não mais necessários</li> <li>• Processos trimestrais para identificar e excluir com segurança os dados do</li> </ul>	<p><b>3.1.a</b> Analise as políticas, processos e procedimentos de retenção e descarte de dados para verificar se incluem, pelo menos, o que segue para todo o armazenamento de dados do titular do cartão (CHD):</p> <ul style="list-style-type: none"> <li>• Limitar a quantia de dados armazenados e o tempo de retenção às restrições conforme exigências legais, regulatórias e/ou comerciais.</li> <li>• Exigências específicas quanto à retenção de dados do titular do cartão (por exemplo, os dados do titular do cartão devem ser retidos pelo período X, por razões comerciais Y).</li> <li>• Exclusão segura dos dados do titular do cartão que não são mais necessários por motivos legais, regulamentares ou comerciais.</li> <li>• Processos trimestrais para identificar e excluir com segurança os dados do titular do cartão que excederem as exigências de retenção definidas.</li> </ul>	<p>Políticas formais de retenção de dados identificam quais dados precisam ser retidos e onde ficam, de forma a serem excluídos ou destruídos com segurança assim que não forem mais necessários.</p> <p>Os únicos dados do titular do cartão que podem ser armazenados são o número da conta principal ou PAN (desde que ilegível), data de vencimento, nome do titular do cartão e código de serviço.</p> <p>É necessário saber onde os dados do titular do cartão estão localizados, para que sejam retidos ou descartados corretamente quando não mais necessários. Para definir os requisitos de retenção adequados, a empresa deverá primeiro conhecer suas necessidades de negócios, bem como as responsabilidades legais e</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>titular do cartão que excederem a retenção definida.</p>	<p><b>3.1.b</b> Converse com os funcionários para verificar se:</p> <ul style="list-style-type: none"> <li>• Todos os locais de armazenamento dos dados do titular do cartão estão incluídos nos processos de retenção e descarte de dados.</li> <li>• Um processo trimestral manual ou automático está implantado para identificar e excluir com segurança os dados do titular do cartão.</li> <li>• O processo trimestral manual ou automático é executado para todos os locais de dados do titular do cartão.</li> </ul>	<p>regulamentares que se aplicam à setor ou ao tipo dos dados que serão retidos.</p>
	<p><b>3.1.c</b> Para obter uma amostra dos componentes do sistema que armazenam dados do titular do cartão:</p> <ul style="list-style-type: none"> <li>• Analise os arquivos e registros do sistema para verificar se os dados armazenados não excedem os requisitos definidos na política de retenção</li> <li>• Observe o mecanismo de exclusão para verificar se os dados são excluídos de forma segura.</li> </ul>	<p>Identificar e excluir dados armazenados que tenham excedido seu período de retenção especificado evita a retenção de dados que não são mais necessários. Este processo pode ser automático ou manual ou uma combinação dos dois. Por exemplo, um procedimento programático (automático ou manual) para localizar e remover dados e/ou uma revisão manual de áreas de armazenamento de dados pode ser realizado.</p> <p>Implementar métodos de exclusão seguros garante que os dados não poderão ser recuperados quando não forem mais necessários.</p> <p><b>Lembre-se: se você não precisar, não os armazene!</b></p>
<p><b>3.2</b> Não armazenar dados de autenticação confidenciais após a autorização (mesmo se estiverem criptografados). Se forem recebidos dados de autenticação confidenciais, processe todos os dados irrecuperáveis ao completar o processo de autorização.</p> <p><i>O armazenamento de dados de</i></p>	<p><b>3.2.a</b> Para os emissores e/ou empresas que suportam serviços de emissão e armazenam dados de autenticação confidenciais, revise as políticas e questione os funcionários para verificar se há justificativa comercial documentada para o armazenamento de dados de autenticação confidenciais.</p>	<p>Os dados de autenticação confidenciais são formados por dados de rastreamento completo, código ou valor de validação do cartão e dados do PIN. O armazenamento de dados de autenticação confidenciais após a autorização é proibido! Esses dados são muito valiosos para indivíduos mal-intencionados, pois permitem falsificar cartões de pagamento e criar transações fraudulentas.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><i>autenticação confidenciais é permitido aos emissores e empresas que suportam serviços de emissão se:</i></p> <ul style="list-style-type: none"> <li>Houver uma justificativa comercial e</li> <li>Os dados são armazenados com segurança.</li> </ul> <p>Os dados de autenticação confidenciais incluem os dados conforme mencionados nos seguintes Requisitos 3.2.1 até 3.2.3:</p>	<p><b>3.2.b</b> Para os emissores e/ou empresas que suportam serviços de emissão e armazenam dados de autenticação confidenciais, analise o armazenamento de dados e configurações do sistema para verificar se os dados de autenticação confidenciais estão seguros.</p>	<p>As entidades que emitem cartões de pagamento ou que desempenham ou suportam serviços de emissão, frequentemente criarão e controlarão os dados de autenticação confidenciais como parte da função de emissão. As empresas que executam, facilitam ou suportam serviços de emissão têm permissão para armazenar dados de autenticação confidenciais SOMENTE SE apresentarem legítima necessidade de negócios para armazenar esses dados.</p> <p>Deve-se observar que todos os requisitos de PCI DSS se aplicam aos emissores e a única exceção para emissores e processadores de emissões é que os dados de autenticação confidenciais poderão ficar retidos se houver uma razão legítima para tanto. Razão legítima é aquela necessária para o desempenho da função fornecida para o emissor e não de conveniência. Esses dados deverão ser armazenados com segurança e de acordo com o PCI DSS e os requisitos específicos da empresa de pagamento.</p>
	<p><b>3.2.c</b> Para todas as outras entidades, se dados de autenticação confidenciais forem recebidos, revise as políticas e procedimentos e analise as configurações do sistema para verificar se os dados não estão retidos após a autorização.</p>	
	<p><b>3.2.d</b> Para todas as outras entidades, se dados de autenticação confidenciais forem recebidos, revise os procedimentos e analise os processos de exclusão dos dados para verificar se os dados são irrecuperáveis.</p>	<p>Para entidades que não executam serviços de emissão, não é permitido reter os dados de autenticação confidenciais após a autorização.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.2.1</b> Não armazene o conteúdo completo de qualquer rastreamento (da tarja magnética localizada na parte posterior do cartão, em dados equivalentes constando no chip ou outro local) após a autorização. Esses dados também são denominados como rastreamento completo, rastreamento, rastreamento 1, rastreamento 2 e dados da tarja magnética.</p> <p><b>Observação:</b> no curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser mantidos:</p> <ul style="list-style-type: none"> <li>• O nome do titular do cartão</li> <li>• O número da conta principal (PAN)</li> <li>• Data de vencimento</li> <li>• O código de serviço</li> </ul> <p>Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.</p>	<p><b>3.2.1</b> Para obter uma amostra dos componentes do sistema, analise as fontes de dados, inclusive, entre outros, o que segue e verifique se o conteúdo completo de qualquer rastreamento da tarja magnética na parte posterior do cartão ou dados equivalentes em um chip não são armazenados após a autorização:</p> <ul style="list-style-type: none"> <li>• Dados de transação de entrada</li> <li>• Todos os registros (por exemplo, transação, histórico, depuração, erro)</li> <li>• Arquivos do histórico</li> <li>• Arquivos de rastreamento</li> <li>• Vários esquemas do banco de dados</li> <li>• Conteúdo de bancos de dados.</li> </ul>	<p>Se os dados de rastreamento completo forem armazenados, os indivíduos mal-intencionados que obtiverem esses dados poderão reproduzir os cartões de pagamento e realizar transações fraudulentas.</p>
<p><b>3.2.2</b> Não armazene o código ou valor de verificação do cartão (o número de três ou quatro dígitos impresso na frente ou no verso do cartão de pagamento usado para verificar transações sem cartão) após a autorização.</p>	<p><b>3.2.2</b> Para obter uma amostra dos componentes do sistema, analise as fontes dos dados, inclusive, entre outros, o que segue e verifique se o código ou o valor de verificação do cartão de três ou quatro dígitos impresso na frente do cartão ou no painel de assinatura (dados CVV2, CVC2, CID, CAV2) não é armazenado após a autorização:</p> <ul style="list-style-type: none"> <li>• Dados de transação de entrada</li> <li>• Todos os registros (por exemplo, transação, histórico, depuração, erro)</li> <li>• Arquivos do histórico</li> <li>• Arquivos de rastreamento</li> <li>• Vários esquemas do banco de dados</li> <li>• Conteúdo de bancos de dados.</li> </ul>	<p>O objetivo do código de validação do cartão é proteger as transações do tipo “cartão não presente”, aquelas feitas por internet, por correio ou telefone (MO/TO), nas quais o consumidor e o cartão não estão presentes.</p> <p>Se esses dados forem roubados, indivíduos mal-intencionados podem executar transações fraudulentas pela internet e por MO/TO.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.2.3</b> Não armazene o número de identificação pessoal (PIN) ou o bloqueio de PIN criptografado após a autorização.</p>	<p><b>3.2.3</b> Para obter uma amostra dos componentes do sistema, analise as informações a seguir e verifique se os PINs e blocos de PIN criptografados não são armazenados após a autorização:</p> <ul style="list-style-type: none"> <li>• Dados de transação de entrada</li> <li>• Todos os registros (por exemplo, transação, histórico, depuração, erro)</li> <li>• Arquivos do histórico</li> <li>• Arquivos de rastreamento</li> <li>• Vários esquemas do banco de dados</li> <li>• Conteúdo de bancos de dados.</li> </ul>	<p>Esses valores só devem ser conhecidos pelo titular do cartão ou pelo banco que emitiu o cartão. Se esses dados forem roubados, indivíduos mal-intencionados podem executar transações fraudulentas de débito protegidas por senha (por exemplo, saques em caixas eletrônicos).</p>
<p><b>3.3</b> Mascarar o PAN quando exibido (os primeiros seis e últimos quatro dígitos são o número máximo de dígitos a serem exibidos), de modo que somente funcionários com necessidade comercial legítima possam visualizar além dos seis primeiros/quatro últimos dígitos do PAN.</p> <p><b>Observação:</b> esse requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do titular do cartão, por exemplo, requisitos legais ou da bandeira do cartão de pagamento para recebimentos do ponto de venda (POS).</p>	<p><b>3.3.a</b> Analise as políticas e procedimentos escritos sobre a mascaramento da exibição de PANs para verificar se:</p> <ul style="list-style-type: none"> <li>• Uma lista de funções que precisam acessar exibições além dos seis primeiros/quatro últimos dígitos (inclui PAN completo) encontra-se documentada, juntamente com a necessidade comercial legítima para que cada função obtenha tal acesso.</li> <li>• O PAN deve ser mascarado quando exibido, como no caso em que apenas funcionários com necessidade comercial legítima podem ver além dos seis primeiros/quatro últimos dígitos do PAN.</li> <li>• Todas as funções não autorizadas especificamente para visualizar o PAN completo devem visualizar apenas PANs mascarados.</li> </ul> <p><b>3.3.b</b> Analise as configurações do sistema para verificar se o PAN completo é exibido apenas para usuários/funções com uma necessidade comercial documentada e que o PAN esteja mascarado para todas as outras solicitações.</p>	<p>A exibição do PAN completo em locais como telas de computador, recibos de cartão de pagamento, faxes ou extratos em papel pode fazer com que esses dados sejam obtidos por indivíduos não autorizados e usados de forma fraudulenta. Garantir que o PAN completo seja exibido apenas para aqueles com necessidade comercial legítima de visualizar o PAN completo minimiza o risco de pessoas não autorizadas obterem acesso aos dados do PAN.</p> <p>A abordagem de mascaramento deve sempre garantir que somente o número mínimo de dígitos seja exibido, conforme necessário, para executar uma função comercial específica. Por exemplo, se apenas os quatro últimos dígitos são necessários para executar uma função comercial, o PAN deve ser mascarado para que os indivíduos que executam a função visualizem</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>3.3.c</b> Analise as exibições do PAN (por exemplo, na tela, em recibos de papel) para verificar se os PANs estão mascarados ao exibir os dados do titular do cartão e se apenas as pessoas com necessidade comercial legítima podem visualizar os seis primeiros/quatro últimos dígitos do PAN.</p>	<p>somente os quatro últimos dígitos. Como outro exemplo, se a função precisa acessar o número de identificação bancária (BIN) para fins de roteamento, desmascarar apenas os dígitos BIN (tradicionalmente, os seis primeiros algarismos) para a função.</p> <p>Este requisito está relacionado à proteção do PAN <u>exibida</u> em telas, recibos, impressões, etc. e não deve ser confundido com o Requisito 3.4 para proteção do PAN quando <u>armazenado</u> em arquivos, bancos de dados, etc.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.4</b> Torne o PAN ilegível em qualquer local onde ele esteja armazenado (inclusive em mídia digital portátil, mídia de backup e em registros) utilizando qualquer uma das seguintes abordagens:</p> <ul style="list-style-type: none"> <li>• Hash de direção única com base na criptografia forte (o hash deve ser do PAN inteiro)</li> <li>• Truncamento (a codificação hash não pode ser usada para substituir o segmento truncado do PAN)</li> <li>• Tokens e blocos de índice (os blocos devem ser armazenados de forma segura)</li> <li>• Criptografia forte com processos e procedimentos de gerenciamento-chave associados.</li> </ul> <p><b>Observação:</b> É um esforço relativamente simples para um indivíduo mal-intencionado reconstituir os dados do PAN original caso ele tenha acesso às versões truncadas e hash do PAN. Onde estiverem presentes versões obscurecidas e truncadas de mesmo PAN no ambiente da</p>	<p><b>3.4.a</b> Analise a documentação sobre o sistema usado para proteger o PAN, incluindo o fornecedor, o tipo de sistema/processo e os algoritmos de criptografia (se aplicável) para verificar se o PAN é apresentado ilegível, usando qualquer um dos métodos a seguir:</p> <ul style="list-style-type: none"> <li>• Codificação hash de direção única com base na criptografia forte</li> <li>• Truncamento</li> <li>• Tokens e blocos de índice, sendo que os blocos são armazenados de forma segura</li> <li>• Criptografia forte com processos e procedimentos de gerenciamento-chave associados.</li> </ul> <p><b>3.4.b</b> Analise as diversas tabelas ou arquivos de um exemplo de repositórios de dados para verificar se o PAN foi tornado ilegível (ou seja, não foi armazenado em texto simples).</p> <p><b>3.4.c</b> Analise um exemplo de mídia removível (por exemplo, fitas de backup) para confirmar se o PAN foi tornado ilegível.</p> <p><b>3.4.d</b> Analise uma amostra dos logs de auditoria, inclusive registros do aplicativo de pagamento, para confirmar que o PAN seja processado de forma ilegível ou não esteja presente nos registros.</p>	<p>Os PANs armazenados no armazenamento principal (bancos de dados ou arquivos simples, como arquivos de texto e planilhas), além de armazenamento não principal (backup, logs de auditoria, logs de exceção ou de resolução de problemas) devem todos estar protegidos.</p> <p>Funções de hash de direção única baseadas em criptografia robusta podem ser usadas para tornar os dados do titular do cartão ilegíveis. As funções de codificação de hash são adequadas quando não houver necessidade de recuperar o número original (o hash de direção única é irreversível). Recomenda-se, porém não se trata de exigência no momento, que um valor de entrada adicional e aleatório seja adicionado aos dados do titular do cartão antes da codificação hash, para reduzir a possibilidade de um invasor comparar os dados (e derivar o PAN) a partir das tabelas de valores de hash previamente computados.</p> <p>O objetivo do truncamento é remover permanentemente um segmento de dados do PAN, de forma que somente uma parte (em geral, sem exceder os primeiro seis e os últimos quatro dígitos) do PAN seja armazenado.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><i>entidade, controles adicionais devem existir para garantir que as versões truncadas e obscurecidas não possam ser correlacionadas para reconstruir o PAN original.</i></p>	<p><b>3.4.e</b> Se as versões truncada e hash do mesmo PAN estiverem presentes no ambiente, analise os controles implementados para garantir que as versões truncada e hash não possam ser correlacionadas para reconstituição do PAN original.</p>	<p>Um token de índice é um token criptográfico que substitui o PAN com base em um determinado índice para um valor imprevisível. Um pad de uso único é um sistema no qual uma chave privada gerada aleatoriamente é usada só uma vez para criptografar uma mensagem que então é decodificada usando um pad e uma chave de uso único correspondentes.</p> <p>O objetivo da criptografia forte (conforme definido no <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>) é que a criptografia se baseie em um algoritmo testado e aceito pela empresa (não um algoritmo “feito em casa”) com chaves de criptografia forte.</p> <p>Ao correlacionar as versões de hash e truncada de um determinado PAN, um indivíduo mal-intencionado poderá facilmente derivar o valor do PAN original. Os controles que evitam a correlação desses dados ajudarão a garantir que o PAN original permaneça ilegível.</p>
<p><b>3.4.1</b> Se a criptografia de dados for utilizada (em vez da criptografia de bancos de dados no nível de arquivo ou coluna), o acesso lógico deve ser gerenciado separadamente e independentemente de mecanismos de controle de acesso e autenticação do sistema operacional nativo (por exemplo, não utilizando bancos de dados de contas de usuário locais ou credenciais gerais de logon da rede). Chaves de decodificação não devem estar associadas a contas de usuários.</p>	<p><b>3.4.1.a</b> Se a criptografia de dados for usada, inspecione a configuração e observe o processo de autenticação para verificar se o acesso lógico aos sistemas de arquivos criptografados foi implementado por meio de um mecanismo que seja separado do mecanismo de autenticação do sistema operacional nativo (por exemplo, não usando os bancos de dados das contas de usuário locais ou credenciais gerais de logon da rede).</p> <p><b>3.4.1.b</b> Observe os processos e questione os funcionários para verificar se as chaves criptográficas são armazenadas de forma segura (por exemplo, armazenadas nas mídias removíveis que estão protegidas adequadamente com controles de acesso robustos).</p>	<p>O objetivo deste requisito é abordar a aceitabilidade da criptografia no nível de disco para tornar os dados do titular do cartão ilegíveis. A criptografia no nível de disco codifica todas os discos/divisões em computador e decodifica automaticamente as informações quando um usuário autorizado as solicita. Muitas soluções de criptografia de dados interceptam as operações de leitura/gravação do sistema operacional e executam as transformações criptográficas adequadas sem nenhuma ação especial por parte do usuário, além de fornecer uma senha ao ligar o sistema ou no início de uma sessão. Com base nessas características de criptografia no nível de</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>Observação:</b> Este requisito aplica-se também a todos os outros requisitos de gerenciamento de chaves e criptografia do PCI DSS.</p>	<p><b>3.4.1.c</b> Analise as configurações e observe os processos para verificar se os dados do titular do cartão nas mídias removíveis estão criptografados onde estiverem armazenados.</p> <p><b>Observação:</b> se a criptografia de dados não for usada para criptografar a mídia removível, os dados armazenados nessa mídia deverão ser tornados ilegíveis por meio de outro método.</p>	<p>disco, a fim de atender a esse requisito, o método não pode:</p> <ol style="list-style-type: none"> <li>1) Utilizar o mesmo autenticador de conta do usuário que o sistema operacional, ou</li> <li>2) Utilizar uma chave de decodificação associada com ou derivada do banco de dados da conta do usuário local do sistema ou credenciais gerais de logon da rede.</li> </ol> <p>A criptografia de dados completa ajuda a proteger os dados no caso de perda de um disco e, portanto, pode ser apropriada para dispositivos portáteis que armazenam dados do titular do cartão.</p>
<p><b>3.5</b> Registre e implemente procedimentos para proteger as chaves utilizadas para armazenar os dados do titular do cartão de forma segura em relação a divulgações ou uso indevido:</p> <p><b>Observação:</b> Esse requisito aplica-se às chaves usadas para proteger dados armazenados do titular do cartão e também às chaves de criptografia de dados; as chaves de criptografia das chaves devem ser, pelo menos, tão fortes quanto as chaves de criptografia dos dados.</p>	<p><b>3.5</b> Analise as políticas e procedimentos de gerenciamento de chave para verificar se os processos estão especificados para proteger as chaves usadas para a criptografia dos dados do titular do cartão contra a divulgação e o uso indevido, e se incluem, pelo menos, o que segue:</p> <ul style="list-style-type: none"> <li>• O acesso às chaves está restrito ao menor número necessário de responsáveis pela proteção.</li> <li>• As chaves de criptografia de chaves são tão fortes quanto as chaves de criptografia de dados que protegem.</li> <li>• As chaves de criptografia de chaves são armazenadas separadamente das chaves de criptografia.</li> <li>• As chaves são armazenadas de forma segura no menor número possível de locais e formatos.</li> </ul>	<p>As chaves criptográficas devem ser muito bem protegidas, pois quem tiver acesso a elas conseguirá decodificar os dados. As chaves de criptografia de chaves, se utilizadas, deverão ser ao menos tão fortes quanto as chaves de criptografia de dados para garantir a proteção adequada da chave que criptografa os dados e dos dados criptografados por essa chave.</p> <p>O requisito para proteger chaves da divulgação e do uso indevido se aplica tanto às chaves de criptografia de dados quanto às chaves de criptografia de chaves. Como uma chave de criptografia de chaves poderá conceder direito de acesso a várias chaves de criptografia de dados, as chaves de criptografia de chaves necessitam de medidas de proteção vigorosas.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.5.1 Requisito adicional, somente para prestadores de serviços:</b> Manter uma descrição documentada da arquitetura criptográfica que inclui:</p> <ul style="list-style-type: none"> <li>• Detalhes de todos os algoritmos, protocolos e chaves usados para a proteção dos dados do titular do cartão, inclusive a força da chave e a data de validade</li> <li>• Descrição do uso da chave para cada chave</li> <li>• Inventário de HSMs e outras SCDs usadas para gerenciamento de chave</li> </ul> <p><b>Observação:</b> Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</p>	<p><b>3.5.1</b> Entrevistar o pessoal responsável e revisar a documentação para verificar se há um documento que descreva a arquitetura criptográfica, incluindo:</p> <ul style="list-style-type: none"> <li>• Detalhes de todos os algoritmos, protocolos e chaves usados para a proteção dos dados do titular do cartão, inclusive a força da chave e a data de validade</li> <li>• Descrição do uso da chave para cada chave</li> <li>• Inventário de HSMs e outras SCDs usadas para gerenciamento de chave</li> </ul>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>Manter atualizada a documentação da arquitetura criptográfica permite à entidade compreender os algoritmos, protocolos e chaves criptográficas usadas para proteger os dados dos titulares do cartão, bem como os dispositivos que geram, usam e protegem as chaves. Isso permite que a entidade mantenha o ritmo em relação ao progresso das ameaças na arquitetura, possibilitando o planejamento das atualizações conforme ocorrem mudanças nos níveis de garantia fornecidos pela potência de diferentes algoritmos/chaves. Manter a documentação também permite à entidade detectar chaves perdidas ou extraviadas ou dispositivos centrais de gerenciamento, bem como identificar adições não autorizadas à arquitetura criptográfica.</p>
<p><b>3.5.2</b> Restrinja o acesso às chaves criptográficas ao menor número necessário de responsáveis pela proteção.</p>	<p><b>3.5.2</b> Analise as listas de acesso aos usuários para verificar se o acesso às chaves está restrito ao menor número necessário de responsáveis pela proteção.</p>	<p>Deve haver pouquíssimas pessoas com acesso às chaves criptográficas (reduzindo o potencial de deixar os dados do titular do cartão visíveis para pessoas não autorizadas), normalmente somente aqueles com responsabilidades pela custódia das chaves.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.5.3</b> Armazene chaves privadas e secretas usadas para criptografar/descodificar os dados do titular do cartão em uma (ou mais) das formas a seguir, em todos os momentos:</p> <ul style="list-style-type: none"> <li>• Criptografadas com uma chave de criptografia de chaves que seja ao menos tão forte quanto a chave de criptografia de dados e que esteja armazenada separadamente da chave de criptografia de dados.</li> <li>• Dentro de um dispositivo criptográfico seguro (por exemplo, um módulo de segurança de hardware (host) (HSM) ou dispositivo de ponto-de-interação aprovado por PTS).</li> <li>• Como duas partes de chave ou componentes de chave de tamanho total, de acordo com um método aceito pela empresa</li> </ul> <p><b>Observação:</b> não é exigido que chaves públicas sejam armazenadas em uma destas formas.</p>	<p><b>3.5.3.a</b> Analise os procedimentos documentados para verificar se as chaves criptográficas usadas para criptografar/descodificar os dados do titular do cartão devem existir em apenas uma (ou mais) das formas a seguir, em todos os momentos.</p> <ul style="list-style-type: none"> <li>• Criptografadas com uma chave de criptografia de chaves que seja ao menos tão forte quanto a chave de criptografia de dados e que esteja armazenada separadamente da chave de criptografia de dados.</li> <li>• Dentro de um dispositivo criptográfico seguro (por exemplo, um módulo de segurança de hardware (host) (HSM) ou dispositivo de ponto-de-interação aprovado por PTS).</li> <li>• Como partes de chave ou componentes de chave, de acordo com um método aceito pela empresa</li> </ul> <p><b>3.5.3.b</b> Analise as configurações do sistema e os locais de armazenamento de chave para verificar se as chaves criptográficas usadas para criptografar/descodificar os dados do titular do cartão existem em uma (ou mais) das formas a seguir, em todos os momentos.</p> <ul style="list-style-type: none"> <li>• Criptografadas com uma chave de criptografia de chave</li> <li>• Dentro de um dispositivo criptográfico seguro (por exemplo, um módulo de segurança de hardware (host) (HSM) ou dispositivo de ponto-de-interação aprovado por PTS).</li> <li>• Como partes de chave ou componentes de chave, de acordo com um método aceito pela empresa</li> </ul> <p><b>3.5.3.c</b> Onde quer que as chaves de criptografia de chave sejam usadas, analise as configurações do sistema e os locais de armazenamento de chave para verificar se:</p> <ul style="list-style-type: none"> <li>• As chaves de criptografia de chaves são tão fortes quanto as chaves de criptografia de dados que protegem</li> <li>• As chaves de criptografia de chaves são armazenadas separadamente das chaves de criptografia.</li> </ul>	<p>Chaves criptográficas devem ser armazenadas com segurança para evitar o acesso não autorizado e desnecessário que poderia resultar na exposição dos dados do titular do cartão.</p> <p>As chaves de criptografia de chaves não precisam ser criptografadas, mas devem ficar protegidas contra divulgação e uso indevido conforme definido no Requisito 3.5. Se forem usadas chaves de criptografia de chave, armazená-las em locais fisicamente e/ou logicamente separados das chaves de criptografia de dados reduz os riscos de acesso não autorizado às duas chaves.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>3.5.4</b> Armazene chaves criptográficas no menor número possível de locais.</p>	<p><b>3.5.4</b> Analise os locais de armazenamento de chave e observe os processos para verificar se as chaves são armazenadas no menor número possível de locais.</p>	<p>Armazenar chaves criptográficas no menor número possível de locais ajuda a organização a acompanhar e monitorar todos os locais de chaves e minimiza o potencial das chaves serem expostas a pessoas não autorizadas.</p>
<p><b>3.6</b> Documente e implemente por completo todos os processos e procedimentos de gerenciamento de chave com relação às chaves criptográficas usadas para a criptografia dos dados do titular do cartão, incluindo o seguinte:</p> <p><b>Observação:</b> <i>Vários padrões do setor para o gerenciamento-chave estão disponíveis a partir de diversos recursos, incluindo NIST, que pode ser encontrado em <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>.</i></p>	<p><b>3.6.a Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Se o prestador de serviços compartilhar chaves com seus clientes para a transmissão ou armazenamento de dados do titular do cartão, analise a documentação que o prestador de serviços fornece aos clientes para verificar se ela inclui uma orientação sobre como transmitir, armazenar e atualizar as chaves do cliente de forma segura, de acordo com os Requisitos 3.6.1 a 3.6.8 abaixo.</p> <p><b>3.6.b</b> Analise os processos e procedimentos de gerenciamento de chave com relação às chaves usadas para a criptografia dos dados do titular do cartão e faça o seguinte:</p>	<p>A forma como as chaves criptográficas são gerenciadas é parte essencial da segurança continuada da solução de criptografia. Um bom processo de gerenciamento de chaves, seja ele manual ou automatizado, como parte do produto de criptografia, baseia-se nos padrões do setor e aborda todos os elementos de chave em 3.6.1 a 3.6.8.</p> <p>Fornecer orientação aos clientes sobre como transmitir, armazenar e atualizar as chaves criptográficas com segurança pode ajudar a evitar que as chaves sejam mal administradas ou divulgadas a entidades não autorizadas.</p> <p>Este requisito aplica-se às chaves utilizadas para criptografar os dados do titular do cartão armazenados e a qualquer chave de criptografia de chaves respectiva.</p> <p><b>Observação:</b> <i>O procedimento de teste 3.6.a é um procedimento adicional que se aplica somente quando a entidade a ser avaliada tratar-se de um prestador de serviços.</i></p>
<p><b>3.6.1</b> Geração de chaves criptográficas fortes</p>	<p><b>3.6.1.a</b> Verifique se os procedimentos de gerenciamento-chave especificam como gerar chaves fortes.</p> <p><b>3.6.1.b</b> Observe os procedimentos para geração de chaves para verificar se as chaves geradas são robustas.</p>	<p>A solução criptográfica deve gerar chaves robustas, conforme definição no <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>, em “Geração de chave criptográfica”. O uso de chaves criptográficas robustas aumenta significativamente o nível de segurança dos dados criptografados do titular do cartão.</p>
<p><b>3.6.2</b> Distribuição segura da chave criptográfica</p>	<p><b>3.6.2.a</b> Verifique se os procedimentos de gerenciamento-chave especificam como distribuir chaves de forma segura.</p>	<p>A solução de criptografia deve distribuir as chaves de forma segura, o que significa que as chaves</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<b>3.6.2.b</b> Observe o método de distribuição de chaves para verificar se elas são distribuídas de forma segura.	são distribuídas somente para os responsáveis identificados em 3.5.1 e nunca distribuídas sem limitação.
<b>3.6.3</b> Armazenamento seguro de chaves criptográficas	<b>3.6.3.a</b> Verifique se os procedimentos de gerenciamento-chave especificam como armazenar chaves de forma segura.  <b>3.6.3.b</b> Observe o método de armazenamento das chaves para verificar se elas estão armazenadas com segurança.	A solução de criptografia deve armazenar as chaves com segurança, por exemplo, criptografando-as com uma chave de criptografia. Armazenar chaves sem a proteção adequada pode implicar no acesso de invasores, resultando na decodificação e exposição dos dados do titular do cartão.
<b>3.6.4</b> Troca de chave criptográfica para as chaves que chegaram ao final de seu cripto-período (por exemplo, após ter passado determinado período de tempo e/ou após certa quantidade de texto cifrado ter sido produzido por dada chave), conforme definido pelo fornecedor associado do aplicativo ou o dono da chave e com base nas práticas recomendadas e orientações do setor (por exemplo, a Publicação Especial NIST 800-57).	<b>3.6.4.a</b> Verifique se os procedimentos de gerenciamento-chave incluem um criptoperíodo definido para cada tipo de chave em uso e se define um processo para modificações de chave no final do criptoperíodo definido.  <b>3.6.4.b</b> Converse com os funcionários para verificar se as chaves são modificadas no final do criptoperíodo definido.	Um cripto-período é o tempo transcorrido durante o qual uma determinada chave de criptografia poderá ser utilizada para seus devidos fins. As considerações para definir o cripto-período incluem, entre outros, a força do algoritmo em destaque, o tamanho ou o comprimento da chave, o risco de comprometimento da chave e a confidencialidade dos dados a serem criptografados.  A troca periódica das chaves de criptografia ao atingirem o cripto-período é essencial para minimizar o risco de alguém obter as chaves de criptografia e usá-las para decodificar os dados.
<b>3.6.5</b> Inutilização ou substituição (por exemplo, arquivamento, destruição e/ou revogação) de chaves consideradas necessárias quando a integridade da chave estiver enfraquecida (por exemplo, saída de um funcionário com conhecimento sobre um componente de chave de texto simples) ou quando houver suspeita de que a chave esteja comprometida.  <b>Observação:</b> Caso chaves criptográficas inutilizadas ou recolocadas precisarem ser retidas, essas chaves deverão ser arquivadas em segurança (por exemplo,	<b>3.6.5.a</b> Verifique se os procedimentos de gerenciamento-chave especificam processos para o que segue: <ul style="list-style-type: none"> <li>• A inutilização ou substituição de chaves quando sua integridade tiver sido enfraquecida</li> <li>• A substituição de chaves que estejam sabidamente ou potencialmente comprometidas.</li> <li>• Qualquer chave mantida após a inutilização ou substituição não são utilizadas para operações de criptografia</li> </ul> <b>3.6.5.b</b> Converse com os funcionários para verificar se os seguintes processos estão implementados: <ul style="list-style-type: none"> <li>• As chaves são inutilizadas ou substituídas quando sua integridade tenha sido enfraquecida, incluindo quando</li> </ul>	Chaves que não são mais usadas nem necessárias ou chaves que se sabe ou são suspeitas de estarem comprometidas devem ser inutilizadas e/ou destruídas para garantir que não possam mais ser usadas. Se for necessário mantê-las (para usar com dados arquivados e criptografados, por exemplo), elas deverão ser muito bem protegidas.  A solução de criptografia deve fornecer e facilitar o processo para substituir as chaves que estejam no prazo de substituição, ou sabidamente ou potencialmente comprometidas.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><i>usando uma chave de criptografia de chaves). Chaves criptográficas arquivadas devem ser usadas somente para fins de decodificação/verificação.</i></p>	<p>alguém com conhecimento sobre a chave sai da empresa.</p> <ul style="list-style-type: none"> <li>• As chaves são substituídas se estiverem sabidamente ou potencialmente comprometidas.</li> <li>• Qualquer chave mantida após a inutilização ou substituição não são utilizadas para operações de criptografia.</li> </ul>	
<p><b>3.6.6</b> Se forem usadas operações manuais de gerenciamento de chave criptográfica de texto simples, essas operações devem ser gerenciadas com o uso de conhecimento separado e de controle duplo.</p> <p><b>Observação:</b> Os exemplos de operações manuais de gerenciamento de chave incluem, entre outros: geração, transmissão, carregamento, armazenamento e destruição de chaves.</p>	<p><b>3.6.6.a</b> Verifique se os procedimentos manuais de gerenciamento-chave de texto simples especificam processos para o uso do que segue:</p> <ul style="list-style-type: none"> <li>• O conhecimento separado de chaves, como os componentes de chaves que estão sob o controle de pelo menos duas pessoas que têm conhecimento apenas de seus próprios componentes de chave; E</li> <li>• Controle duplo de chaves, que necessita de pelo menos duas pessoas para executar qualquer operação de gerenciamento-chave e que uma única pessoa não tenha acesso aos materiais de autenticação (por exemplo, senhas ou chaves) do outro.</li> </ul> <p><b>3.6.6</b> Converse com os funcionários e/ou observe os processos para verificar se as chaves manuais de texto simples são gerenciadas com:</p> <ul style="list-style-type: none"> <li>• Conhecimento separado, E</li> <li>• Controle duplo</li> </ul>	<p>O conhecimento separado e o controle duplo das chaves são usados para eliminar a possibilidade de uma pessoa ter acesso à chave inteira. Este controle é aplicável em operações de gerenciamento de chaves manual ou onde o gerenciamento de chaves não for implementado por um produto de criptografia.</p> <p>Conhecimento separado é um método segundo o qual duas ou mais pessoas possuem componentes de chave separadamente, em que cada pessoa conhece apenas seu próprio componente e os componentes de chave individuais não transmitem nenhum conhecimento da chave criptográfica original.</p> <p>O controle duplo requer que duas ou mais pessoas realizem uma função e uma única pessoa não pode acessar ou usar os materiais de autenticação do outro.</p>
<p><b>3.6.7</b> Prevenção contra a substituição não autorizada de chaves criptográficas.</p>	<p><b>3.6.7.a</b> Verifique se os procedimentos do gerenciamento de chaves especificam processos para evitar a substituição não autorizada das chaves.</p> <p><b>3.6.7.b</b> Converse com os funcionários e/ou observe os processos para verificar se a substituição não autorizada de chaves é evitada.</p>	<p>A solução de criptografia não deve permitir nem aceitar a substituição de chaves vindas de fontes não autorizadas ou de processos inesperados.</p>
<p><b>3.6.8</b> Requisito para que os responsáveis pela proteção das chaves criptográficas assinem um formulário declarando que eles compreendem e aceitam suas responsabilidades pela proteção das</p>	<p><b>3.6.8.a</b> Verifique se os procedimentos do gerenciamento de chaves especificam processos para que os responsáveis pela proteção garantam (por escrito ou eletronicamente) que compreendem e aceitam suas responsabilidades de proteção das chaves.</p>	<p>Este processo garantirá que os indivíduos que atuam como responsáveis se comprometam com a função de responsáveis pela chave e conheçam e aceitem as responsabilidades.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
chaves.	<b>3.6.8.b</b> Observe a documentação ou outras evidências que demonstrem se os responsáveis pela proteção garantem (por escrito ou eletronicamente) que compreendem e aceitam suas responsabilidades de proteção das chaves.	
<b>3.7</b> Certifique-se de que as políticas de segurança e os procedimentos operacionais para proteger os dados armazenados do titular do cartão estejam documentados, em uso e que sejam conhecidos por todas as partes envolvidas.	<b>3.7</b> Analise a documentação e converse com os funcionários para verificar se as políticas de segurança e os procedimentos operacionais para proteção dos dados armazenados do titular do cartão estão: <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	Os funcionários devem estar cientes e seguir as políticas de segurança e os procedimentos operacionais documentados para gerenciar o armazenamento seguro dos dados do titular do cartão continuamente.

## Requisito 4: Criptografar a transmissão de dados do titular do cartão em redes abertas e públicas

As informações confidenciais devem ser criptografadas durante a transmissão nas redes que são facilmente acessadas por indivíduos mal-intencionados. Redes sem fio configuradas de forma incorreta e vulnerabilidades na criptografia herdada e nos protocolos de autenticação permanecem como alvos contínuos de indivíduos mal-intencionados que exploram vulnerabilidades para obtenção de acesso privilegiado aos ambientes de dados do titular do cartão.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>4.1</b> Usar protocolos de segurança e criptografia robusta para proteger dados confidenciais do titular do cartão durante a transmissão em redes abertas e públicas, incluindo os seguintes:</p> <ul style="list-style-type: none"> <li>Somente chaves e certificados confiáveis são aceitos.</li> <li>O protocolo em uso suporta apenas versões ou configurações seguras.</li> <li>A força da criptografia é adequada para a metodologia de criptografia que está sendo utilizada.</li> </ul> <p><b>Observação:</b> Onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.</p>	<p><b>4.1.a</b> Identifique todos os locais onde os dados do titular do cartão são transmitidos ou recebidos por redes públicas e abertas. Analise os padrões documentados e compare com as configurações do sistema para verificar o uso de protocolos de segurança e criptografia forte em todos os locais.</p> <p><b>4.1.b</b> Revise as políticas e procedimentos documentados para verificar se os processos são especificados para o que segue:</p> <ul style="list-style-type: none"> <li>Aceitação de apenas chaves e/ou certificados confiáveis</li> <li>O protocolo em uso suporta apenas versões e configurações seguras (versões e configurações não seguras não são suportadas)</li> <li>Implementação de força de criptografia adequada conforme a metodologia de criptografia que está sendo utilizada.</li> </ul>	<p>As informações confidenciais devem ser criptografadas durante a transmissão por redes públicas, pois é fácil e comum para um indivíduo mal-intencionado interceptar e/ou desviar os dados enquanto eles estiverem em trânsito.</p> <p>A transmissão segura dos dados do titular do cartão requer o uso de chaves/certificados confiáveis, um protocolo seguro para o transporte e criptografia robusta adequada para criptografar dados do titular do cartão. As solicitações de conexão de sistemas que não suportam a criptografia forte adequada e que possam resultar em uma conexão não segura, não devem ser aceitas.</p> <p>Observe que algumas implementações de protocolo (como SSL SSH v1.0 e antigo TLS) possuem vulnerabilidades conhecidas que podem ser usadas por um invasor para obter controle do sistema afetado. Seja qual for o protocolo de segurança usado, certifique-se de que esteja configurado para uso somente em configurações e versões seguras, a fim de impedir o uso de conexão insegura — por exemplo, ao usar apenas certificados confiáveis com suporte para criptografia robusta (sem suporte para protocolos ou métodos inseguros ou fracos).</p>
<p>Os exemplos de redes abertas e públicas incluem, entre outros:</p> <ul style="list-style-type: none"> <li>A internet</li> <li>Tecnologias sem fio, incluindo 802.11 e Bluetooth</li> <li>Tecnologia celular, por exemplo, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA)</li> <li>General Packet Radio Service (GPRS)</li> <li>Comunicações de satélite</li> </ul>	<p><b>4.1.c</b> Selecione e observe uma amostra das transmissões de entrada e saída conforme ocorrem (por exemplo, pela observação de processos do sistema ou tráfego de rede), para verificar se os dados do titular do cartão utilizam criptografia robusta durante o trânsito.</p> <p><b>4.1.d</b> Analise as chaves e certificados para verificar se somente chaves e/ou certificados confiáveis são aceitos.</p> <p><b>4.1.e</b> Analise as configurações do sistema para verificar se o protocolo foi implementado para usar apenas configurações seguras e se não suportam versões ou configurações não seguras.</p>	<p>Verificar se os certificados são confiáveis (por exemplo, que não estejam vencidos e que sejam emitidos a partir de uma fonte confiável) ajuda a garantir a integridade da conexão segura.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>4.1.f</b> Analise as configurações do sistema para verificar se a força da criptografia adequada é implementada para a metodologia de criptografia que está sendo utilizada. (Verifique as recomendações/práticas recomendadas do fornecedor.)</p> <p><b>4.1.g</b> Para as implementações TLS, analise as configurações do sistema para verificar se o TLS está habilitado sempre que os dados do titular do cartão forem transmitidos ou recebidos.</p> <p>Por exemplo, para implementações com base no navegador:</p> <ul style="list-style-type: none"> <li>• O “HTTPS” aparece como parte do protocolo de Universal Record Locator (URL) do navegador, e</li> <li>• Os dados do titular do cartão são exigidos somente se o “HTTPS” aparece como parte do URL.</li> </ul> <p><b>4.1.h</b> Se o SSL/TLS antigo estiver em uso, executar os procedimentos de teste previstos no <i>Apêndice A2: Requisitos adicionais do PCI DSS para entidades que usam SSL/TLS antigo.</i></p>	<p>Geralmente, o URL da página Web inicia com “HTTPS” e/ou o navegador da Web exibe um ícone de cadeado em algum lugar na janela do navegador. Muitos fornecedores de certificados TLS também fornecem um selo de verificação amplamente visível (às vezes, denominado “selo de segurança”, “selo de site seguro” ou “selo confiável seguro”), com a possibilidade de clicarmos no selo para exibição das informações sobre o site.</p> <p>Consultar os padrões e as práticas recomendadas para o setor para obter informações sobre criptografia robusta e protocolos de segurança (p. ex., NIST SP 800-52 e SP 800-57, OWASP etc.)</p>
<p><b>4.1.1</b> Certifique-se de que as redes sem fio estejam transmitindo dados do titular do cartão ou estejam conectadas ao ambiente de dados do titular do cartão, siga as práticas recomendadas pelo setor para implementar a criptografia robusta na autenticação e transmissão.</p>	<p><b>4.1.1</b> Identifique todas as redes sem fio que transmitem dados do titular do cartão ou conectadas ao ambiente de dados do titular do cartão. Analise os padrões documentados e compare com as configurações do sistema para verificar o que segue para todas as redes sem fio identificadas:</p> <ul style="list-style-type: none"> <li>• As práticas recomendadas pelo setor são usadas para implementar criptografia robusta na autenticação e na transmissão.</li> <li>• A criptografia fraca (por exemplo, WEP e SSL) não é utilizada como controle de segurança para autenticação ou transmissão.</li> </ul>	<p>Usuários mal-intencionados usam as várias ferramentas que estão disponíveis gratuitamente para espionar as comunicações sem fio. O uso de criptografias fortes pode limitar a divulgação de informações confidenciais através da rede sem fio.</p> <p>A criptografia robusta para autenticação e transmissão dos dados do titular do cartão é necessária para evitar que usuários mal-intencionados obtenham acesso à rede sem fio ou utilizem as redes sem fio para acessar outros dados ou redes internos.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>4.2</b> Jamais envie PANs desprotegidos por tecnologias de envio de mensagens ao usuário final (por exemplo, email, mensagens instantâneas, SMS, chat etc.).</p>	<p><b>4.2.a</b> Se forem utilizadas tecnologias de mensagem ao usuário final para enviar dados do titular do cartão, observe os processos de envio do PAN e analise uma amostra das transmissões de saída quando ocorrerem, para verificar se o PAN entregue está ilegível ou protegido com criptografia robusta sempre que for enviado com o uso de tecnologias de mensagens ao usuário final.</p> <p><b>4.2.b</b> Revise as políticas escritas para verificar a existência de uma política que afirme que os PANs desprotegidos não devem ser enviados por meio das tecnologias de envio de mensagens de usuário final.</p>	<p>Email, mensagens instantâneas, SMS e chat podem ser facilmente interceptados por sniffing de pacotes durante a entrega por redes internas e públicas. Não utilize essas ferramentas de envio de mensagem para enviar o PAN se elas não estiverem configuradas para fornecer criptografia forte.</p> <p>Além disso, se uma entidade solicitar PAN via tecnologias de mensagens ao usuário final, a entidade deve fornecer uma ferramenta ou método para proteção de PANs usando criptografia robusta ou tornando os PANs ilegíveis antes da transmissão.</p>
<p><b>4.3</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para criptografar as transmissões dos dados do titular do cartão estejam documentados, em uso e sejam conhecidos por todas as partes envolvidas.</p>	<p><b>4.3</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e os procedimentos operacionais para criptografar as transmissões dos dados do titular do cartão estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários devem estar cientes e seguir as políticas de segurança e os procedimentos operacionais para gerenciar a transmissão segura dos dados do titular do cartão continuamente.</p>

## Manter um programa de gerenciamento de vulnerabilidades

### **Requisito 5: Proteja todos os sistemas contra softwares prejudiciais e atualize regularmente programas ou software de antivírus**

Softwares mal-intencionados, normalmente chamados de “malware” (incluindo vírus, worms e cavalos de Troia) adentram a rede durante muitas atividades de negócios aprovadas, incluindo e-mail dos funcionários e uso da internet, computadores móveis e dispositivos de armazenamento, resultando na exploração das vulnerabilidades do sistema. O software de antivírus deve ser usado em todos os sistemas comumente afetados pelo malware para proteger os sistemas de ameaças atuais e potenciais de softwares mal-intencionados. Soluções adicionais contra malware podem ser consideradas como suplemento ao software de antivírus; no entanto, estas soluções adicionais não substituem a necessidade do software de antivírus estar adequado.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>5.1</b> Implemente softwares de antivírus em todos os sistemas normalmente afetados por softwares mal-intencionados (especialmente em computadores pessoais e servidores).</p>	<p><b>5.1</b> Para obter uma amostra dos componentes do sistemas incluindo todos os tipos de sistemas operacionais normalmente afetados por softwares mal-intencionados, verifique se o software de antivírus foi implementado se houver uma tecnologia antivírus aplicável.</p>	<p>Existe um fluxo constante de invasões usando façanhas amplamente divulgadas, muitas vezes do tipo “zero day” (uma invasão que se aproveita de uma vulnerabilidade previamente desconhecida), contra sistemas até então seguros. Sem uma solução de antivírus que seja atualizada regularmente, essas novas formas de software mal-intencionado podem atacar os sistemas, desativar uma rede ou levar ao comprometimento dos dados.</p>
<p><b>5.1.1</b> Certifique-se de que os programas antivírus sejam capazes de detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados.</p>	<p><b>5.1.1</b> Revise a documentação do fornecedor e analise as configurações do antivírus para verificar se os programas antivírus;</p> <ul style="list-style-type: none"> <li>• Detectam todos os tipos conhecidos de softwares mal-intencionados,</li> <li>• Removem todos os tipos conhecidos de softwares mal-intencionados, e</li> <li>• Protegem contra todos os tipos conhecidos de softwares mal-intencionados.</li> </ul> <p><i>Os exemplos de tipos de softwares mal-intencionados incluem vírus, worms, trojans, spyware, adware e rootkits.</i></p>	<p>É importante proteger contra <b>TODOS</b> os tipos e formas de softwares mal-intencionados.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>5.1.2</b> Para sistemas que normalmente não são atacados por softwares mal-intencionados, execute avaliações periódicas para identificar e avaliar a evolução de ameaças de malware a fim de confirmar se tais sistemas continuam a não precisar de software de antivírus.</p>	<p><b>5.1.2</b> Converse com os funcionários para verificar se a evolução de ameaças de malware é monitorada e avaliada para sistemas que normalmente não são atacados por softwares mal-intencionados, a fim de confirmar se tais sistemas continuam a não precisar de software de antivírus.</p>	<p>Tipicamente, mainframes, computadores de médio porte (como AS/400) e sistemas similares podem não ser alvos ou afetados por malware no momento. No entanto, as tendências do setor para softwares mal-intencionados podem mudar rapidamente, por isso é importante que as organizações estejam cientes de novos malwares que possam afetar seus sistemas, por exemplo, monitorando os avisos de segurança do fornecedor e novos grupos de antivírus para determinar se seus sistemas podem estar sob ameaça de novos malwares.</p> <p>As tendências em softwares mal-intencionados devem ser incluídas na identificação de novas vulnerabilidades de segurança e os métodos para resolver novas tendências devem ser incorporados aos padrões de configuração da empresa e aos mecanismos de proteção, conforme necessário</p>
<p><b>5.2</b> Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue:</p> <ul style="list-style-type: none"> <li>• São mantidos atualizados</li> <li>• Executam varreduras periódicas</li> <li>• Geram logs de auditoria que são mantidos conforme o Requisito 10.7 do PCI DSS.</li> </ul>	<p><b>5.2.a</b> Analise as políticas e os procedimentos para verificar se é exigido que as definições e o software de antivírus sejam mantidos atualizados.</p> <p><b>5.2.b</b> Analise as configurações do antivírus, incluindo a instalação principal do software para verificar se os mecanismos antivírus estão:</p> <ul style="list-style-type: none"> <li>• Configurados para executar atualizações automáticas, e</li> <li>• Configurados para executar varreduras periódicas.</li> </ul> <p><b>5.2.c</b> Analise uma amostra dos componentes do sistema incluindo todos os tipos de sistemas operacionais normalmente afetados pelos softwares mal-intencionados, para verificar se:</p> <ul style="list-style-type: none"> <li>• O software de antivírus e as definições são atuais.</li> <li>• Executam varreduras periódicas.</li> </ul>	<p>Mesmo as melhores soluções antivírus são limitadas se não forem atualizadas com as mais recentes atualizações de segurança, arquivos de assinatura ou proteções contra malware.</p> <p>Os logs de auditoria oferecem a capacidade de monitorar as atividades do vírus e de malware e as reações contra malware. Dessa forma, é imprescindível que as soluções de malware sejam configuradas de forma a gerar logs de auditoria e esses logs deverão ser gerenciados de acordo com o Requisito 10.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>5.2.d</b> Analise as configurações do antivírus, incluindo a instalação principal do software e uma amostra dos componentes do sistema para verificar se:</p> <ul style="list-style-type: none"><li>• A geração de log do software de antivírus está habilitada, e</li><li>• Os logs são mantidos de acordo com o Requisito 10.7 do PCI DSS.</li></ul>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>5.3</b> Certifique-se de que os mecanismos antivírus estejam funcionando ativamente e não possam ser desativados ou alterados pelos usuários, a menos que seja especificamente autorizado pelo gerenciamento com base em cada caso por um período limitado de tempo.</p> <p><b>Observação:</b> <i>as soluções de antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período de tempo durante o qual a proteção antivírus não estiver ativa.</i></p>	<p><b>5.3.a</b> Analise as configurações do antivírus, incluindo a instalação principal do software e uma amostra dos componentes do sistema para verificar se o software de antivírus está funcionando ativamente.</p> <p><b>5.3.b</b> Analise as configurações do antivírus, incluindo a instalação principal do software e uma amostra dos componentes do sistema para verificar se o software de antivírus não pode ser desativado ou modificado pelos usuários.</p> <p><b>5.3.c</b> Converse com os funcionários responsáveis e observe os processos para verificar se o software de antivírus não pode ser desativado ou alterado pelos usuários, a menos que seja especificamente autorizado pelo gerenciamento com base em cada caso por um período limitado de tempo.</p>	<p>O antivírus executado continuamente e que é desativado para ser modificado proporcionará a segurança persistente contra malware.</p> <p>O uso de controles baseados na política em todos os sistemas para garantir que as proteções contra malware não possam ser modificadas ou desativadas ajudará a evitar que a fraqueza do sistema seja aproveitada por software mal-intencionado.</p> <p>Medidas adicionais de segurança também podem ser necessárias pelo período de tempo durante o qual a proteção antivírus não estiver ativada, por exemplo, desconectar o sistema desprotegido da internet enquanto a proteção antivírus estiver desativada e executar uma varredura completa depois que ela for reativada.</p>
<p><b>5.4</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para proteger os sistemas contra malware estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>5.4</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e procedimentos operacionais para proteger os sistemas contra malware estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para garantir que os sistemas estejam continuamente protegidos contra malware.</p>

## Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

Indivíduos inescrupulosos usam as vulnerabilidades da segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são solucionadas pelos patches de segurança disponibilizados pelos fornecedores, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os sistemas devem contar com os patches de software adequados para proteção contra a exploração e o comprometimento dos dados do titular do cartão por indivíduos e softwares mal-intencionados.

**Observação:** Patches de software adequados são aqueles patches que foram avaliados e testados de forma suficiente para determinar se os patches não entram em conflito com as configurações de segurança existentes. Para aplicativos desenvolvidos internamente, diversas vulnerabilidades podem ser evitadas ao utilizar processos de desenvolvimento do sistema padrão e técnicas de codificação seguras.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.1</b> Estabeleça um processo para identificar as vulnerabilidades de segurança, usando fontes externas de boa reputação para informações de vulnerabilidades da segurança e classifique uma escala de risco (por exemplo, “alto”, “médio” ou “baixo”) para vulnerabilidades de segurança recentemente descobertas.</p> <p><b>Observação:</b> as classificações de risco devem ser baseadas nas práticas recomendadas pelo setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.</p> <p>Os métodos para avaliar as vulnerabilidades e classificar o nível de risco variam baseados no ambiente da organização e na estratégia de avaliação de risco. As classificações de risco devem, no mínimo, identificar todas as vulnerabilidades consideradas de “alto risco” ao ambiente. Além da classificação de risco, as vulnerabilidades podem ser consideradas “críticas” se apresentarem uma ameaça iminente ao ambiente, sistemas críticos de impacto e/ou resultariam em comprometimento potencial se não</p>	<p><b>6.1.a</b> Analise as políticas e procedimentos para verificar se os processos estão definidos para o que segue:</p> <ul style="list-style-type: none"> <li>• Para identificar novas vulnerabilidades da segurança</li> <li>• Para classificar uma escala de risco para as vulnerabilidades que incluem identificação de todas as vulnerabilidades de “alto risco” e “críticas”.</li> <li>• Para usar fontes externas de boa reputação para obter informações sobre vulnerabilidade da segurança.</li> </ul> <p><b>6.1.b</b> Converse com os funcionários responsáveis e observe os processos para verificar se:</p> <ul style="list-style-type: none"> <li>• Novas vulnerabilidades da segurança são identificadas.</li> <li>• Uma escala de risco é classificada para vulnerabilidades que incluem identificação de todas as vulnerabilidades de “alto risco” e “críticas”.</li> <li>• Os processos de identificação de novas vulnerabilidades de segurança incluem o uso de fontes externas de boa reputação para obtenção de informações sobre vulnerabilidades.</li> </ul>	<p>O objetivo deste requisito é que as organizações se mantenham atualizadas quanto a novas vulnerabilidades que poderão interferir no sistema.</p> <p>As fontes de informação de vulnerabilidades devem ser confiáveis e frequentemente incluem sites do fornecedor, novos grupos do setor, lista de envios ou RSS feeds.</p> <p>Quando uma organização identifica uma vulnerabilidade que poderá afetar seu ambiente, o risco que essa vulnerabilidade representa deve ser avaliado e classificado. A organização deve então, ter um método adequado para avaliar as vulnerabilidades continuamente e classificar as escalas de risco para estas vulnerabilidades. Isso não acontece pela varredura ASV ou varredura de vulnerabilidade interna, mas exige um processo para monitorar ativamente as fontes do setor para informações de vulnerabilidade.</p> <p>Classificar os riscos (por exemplo, como “altos”, “médios” ou “baixos”) permite que as organizações identifiquem, priorizem e encaminhem itens de maior risco mais rapidamente e reduzam a probabilidade de as vulnerabilidades que representarem maior risco serem exploradas.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><i>resolvidas. Exemplos de sistemas críticos podem incluir sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão.</i></p>		
<p><b>6.2</b> Certifique-se de que todos os componentes do sistema e softwares estejam protegidos de vulnerabilidades conhecidas instalando os patches de segurança aplicáveis disponibilizados pelos fornecedores. Instale patches de segurança críticos em até um mês após o lançamento.</p> <p><b>Observação:</b> os patches de segurança crítica devem ser identificados de acordo com o processo de classificação de risco definido no Requisito 6.1.</p>	<p><b>6.2.a</b> Analise as políticas e procedimentos relacionados à instalação dos patches de segurança para verificar se estão definidos processos para:</p> <ul style="list-style-type: none"> <li>• Instalação de patches de segurança críticos disponibilizados pelo fornecedor em até um mês após o lançamento.</li> <li>• Instalação de todos os patches de segurança aplicáveis disponibilizados pelo fornecedor dentro de um período de tempo apropriado (por exemplo, dentro de três meses).</li> </ul> <p><b>6.2.b</b> Para obter uma amostra dos componentes do sistema e dos softwares relacionados, compare a lista de patches de segurança instalados em cada sistema com a lista de patches de segurança mais recentes do fornecedor para verificar o seguinte:</p> <ul style="list-style-type: none"> <li>• Os patches de segurança críticos disponibilizados pelo fornecedor são instalados em até um mês após o lançamento.</li> <li>• Todos os patches de segurança aplicáveis disponibilizados pelo fornecedor são instalados em um período de tempo apropriado (por exemplo, dentro de três meses).</li> </ul>	<p>Existe um fluxo constante de invasões usando façanhas amplamente divulgadas, muitas vezes do tipo “zero day” (uma invasão que se aproveita de uma vulnerabilidade previamente desconhecida), contra sistemas até então seguros. Se os patches mais recentes não forem implantados nos sistemas críticos assim que possível, um indivíduo mal-intencionado pode usá-los para atacar ou desativar um sistema ou obter acesso aos dados confidenciais.</p> <p>Priorizar os patches para a infraestrutura crítica garante que os sistemas e dispositivos de alta prioridade sejam protegidos contra vulnerabilidades assim que o patch é lançado. Considere priorizar as instalações do patch de forma que os patches de segurança em sistemas críticos ou em risco sejam instalados em até 30 dias e outros patches de menor risco sejam instalados em 2 ou 3 meses.</p> <p>Este requisito destina-se aos patches aplicáveis para todo software instalado, inclusive aplicativos de pagamento (tanto validados, como não validados para PA-DSS).</p>
<p><b>6.3</b> Desenvolva aplicativos de software internos e externos (incluindo acesso administrativo pela Web aos aplicativos) com segurança, conforme segue:</p> <ul style="list-style-type: none"> <li>• De acordo com o PCI DSS (por exemplo, autenticação e logs seguros)</li> <li>• Baseados nos padrões e/ou práticas recomendadas pelo setor.</li> <li>• Incorporar segurança da informação ao longo da vida útil do desenvolvimento do</li> </ul>	<p><b>6.3.a</b> Analise os processos de desenvolvimento do software por escrito para verificar se os processos foram baseados nos padrões e/ou nas práticas recomendadas pelo setor.</p> <p><b>6.3.b</b> Analise os processos de desenvolvimento do software por escrito para verificar se a segurança da informação foi incluída durante o ciclo de vida.</p> <p><b>6.3.c</b> Analise os processos de desenvolvimento do software por escrito para verificar se os aplicativos de software foram desenvolvidos de acordo com o PCI DSS.</p>	<p>Sem a inclusão de uma proteção durante as fases de definição de requisitos, design, análise e teste do desenvolvimento de software, as vulnerabilidades de segurança podem ser apresentadas de forma inadvertida ou mal-intencionada no ambiente de produção.</p> <p>Saber como os dados confidenciais são controlados pelo aplicativo (incluindo quando são armazenados, transmitidos e quando estão na memória) pode ajudar a identificar onde os dados precisam ser</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>software.</p> <p><b>Observação:</b> <i>isso se aplica a todos os softwares desenvolvidos internamente, bem como a softwares personalizados ou sob encomenda desenvolvidos por terceiros.</i></p>	<p><b>6.3.d</b> Converse com os desenvolvedores do software para verificar se processos por escrito de desenvolvimento do software estão implementados.</p>	<p>protegidos.</p>
<p><b>6.3.1</b> Remova as contas de desenvolvimento, teste e/ou personalizados, IDs de usuário e senhas antes que o aplicativo se torne ativo ou seja lançado aos clientes.</p>	<p><b>6.3.1</b> Analise os procedimentos escritos do desenvolvimento do software e questione os funcionários responsáveis para verificar se as contas de pré-produção e/ou de aplicativos personalizados, IDs de usuários e/ou senhas são removidos antes de um aplicativo ser produzido ou lançado aos clientes.</p>	<p>Contas de desenvolvimento, teste e/ou aplicativos personalizados, IDs de usuários e senhas devem ser removidos do código de produção antes de o aplicativo ser ativado ou liberado para os clientes, pois esses itens podem fornecer informações sobre o funcionamento do aplicativo. A posse dessas informações pode facilitar o comprometimento do aplicativo e dos dados relacionados ao titular do cartão.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.3.2</b> Revise o código personalizado antes da liberação para produção ou clientes a fim de identificar qualquer possível vulnerabilidade no código (usando processos manuais ou automatizados) para incluir ao menos o seguinte:</p> <ul style="list-style-type: none"> <li>• As alterações dos códigos são analisadas por outras pessoas além do autor do código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras.</li> <li>• As revisões de código garantem que o código seja desenvolvido de acordo com as diretrizes de codificação seguras.</li> <li>• As correções adequadas são implementadas antes da liberação.</li> <li>• Os resultados das análises dos códigos são revisados e aprovados pelo gerenciamento antes da liberação.</li> </ul> <p><i>(Continua na próxima página)</i></p>	<p><b>6.3.2.a</b> Analise os procedimentos escritos do desenvolvimento do software e questione os funcionários responsáveis para confirmar se todas as alterações nos códigos dos aplicativos personalizados devem ser revisadas (usando processos manuais ou automatizados), conforme segue:</p> <ul style="list-style-type: none"> <li>• As alterações dos códigos são analisadas por outras pessoas além do autor que originou o código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras.</li> <li>• As análises dos códigos asseguram que o código foi desenvolvido de acordo com as diretrizes de codificação seguras (consulte o Requisito 6.5 do PCI DSS).</li> <li>• As correções adequadas são implementadas antes da liberação.</li> <li>• Os resultados das análises dos códigos são revisados e aprovados pelo gerenciamento antes da liberação.</li> </ul>	<p>As vulnerabilidades de segurança no código personalizado são comumente exploradas por indivíduos mal-intencionados para obter acesso a uma rede e comprometer os dados do titular do cartão.</p> <p>Um indivíduo com conhecimento e experiência nas técnicas de análise do código deve estar envolvido no processo de análise. As análises do código devem ser realizadas por alguém que não seja o desenvolvedor do código a fim de permitir uma revisão independente e objetiva. Processos ou ferramentas automatizados também podem ser usados ao invés de análises manuais, mas pode ser difícil ou até mesmo impossível para uma ferramenta automatizada identificar alguns problemas do código.</p> <p>Corrigir os erros de codificação antes que o código seja enviado para produção ou distribuído para os clientes evita que o mesmo exponha os ambientes a possíveis aproveitadores. Também é muito mais difícil de resolver um código com defeito depois de ele ser distribuído ou liberado para ambientes de produção.</p> <p>Incluir uma revisão formal e aprovação do gerenciamento antes da liberação ajuda a garantir que o código seja aprovado e tenha sido desenvolvido de acordo com as políticas e procedimentos.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>Observação:</b> Este requisito referente às análises dos códigos se aplica a todos os códigos personalizados (internos e voltados ao público), como parte integrante do ciclo de vida de desenvolvimento do sistema.</p> <p>As análises dos códigos podem ser realizadas por equipes internas instruídas ou terceiros. Os aplicativos da Web voltados ao público também estão sujeitos a controles extras para abranger ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.6 do PCI DSS.</p>	<p><b>6.3.2.b</b> Selecione uma amostra de alterações recentes dos aplicativos personalizados e verifique se o código do aplicativo personalizado é analisado de acordo com o item 6.3.2.a acima.</p>	
<p><b>6.4</b> Siga os procedimentos de controle de alterações para todas as alterações nos componentes do sistema. Esses processos devem incluir o seguinte:</p>	<p><b>6.4</b> Analise as políticas e os procedimentos para verificar se o seguinte está definido:</p> <ul style="list-style-type: none"> <li>• Os ambientes de desenvolvimento/teste são separados do ambiente de produção, com controle de acesso implementado para executar a separação.</li> <li>• Uma separação das tarefas entre a equipe atribuída aos ambientes de desenvolvimento/teste e a atribuída ao ambiente de produção.</li> <li>• Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento.</li> <li>• Os dados e as contas de teste são removidos antes que o sistema de produção se torne ativo.</li> <li>• Os procedimentos de controle de alterações ligados à implementação de patches de segurança e às modificações estão documentados.</li> </ul>	<p>Sem controles de alteração adequadamente documentados e implementados, os recursos de segurança podem ser omitidos sem ou com intenção ou ainda tornados inoperáveis e podem ocorrer irregularidades no processamento ou pode ser introduzido um código mal-intencionado.</p>
<p><b>6.4.1</b> Separe os ambientes de teste/desenvolvimento do ambiente de produção e reforce a separação com controle de acesso.</p>	<p><b>6.4.1.a</b> Analise a documentação de rede e as configurações do dispositivo de rede para verificar se os ambientes de desenvolvimento/teste são separados do ambiente de produção.</p> <p><b>6.4.1.b</b> Analise os ajustes dos controles de acesso para verificar se estes estão implementados para forçar a separação entre os ambientes de teste/desenvolvimento e os ambientes de produção.</p>	<p>Devido à mutação constante dos ambientes de desenvolvimento e teste, estes tendem a ser menos seguros do que o ambiente de produção. Sem a separação adequada entre os ambientes, o ambiente de produção e os dados do titular do cartão podem tornar-se comprometidos, em razão das configurações de segurança menos rigorosas e possíveis vulnerabilidades em um ambiente de teste ou desenvolvimento.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.4.2</b> Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção</p>	<p><b>6.4.2</b> Observe os processos e questione os funcionários designados para os ambientes de teste/desenvolvimento e os designados para os ambientes de produção para verificar se a separação dos deveres foi implementada entre eles.</p>	<p>Reduzir o número de pessoas com acesso ao ambiente de produção e aos dados do titular do cartão reduz os riscos e contribui para garantir que o acesso seja limitado aos indivíduos com necessidade comercial de conhecimento.</p> <p>O objetivo deste requisito é separar as funções de desenvolvimento e teste das funções de produção. Por exemplo, um desenvolvedor poderá utilizar uma conta com nível de administrador com privilégios elevados no ambiente de desenvolvimento e possuir uma conta separada com acesso de nível de usuário ao ambiente de produção.</p>
<p><b>6.4.3</b> Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento</p>	<p><b>6.4.3.a</b> Observe os processos de teste e questione os funcionários para verificar se os procedimentos estão implementados para garantir que os dados de produção (PANs ativos) não sejam usados para testes ou desenvolvimento.</p> <p><b>6.4.3.b</b> Analise uma amostra dos dados de teste para verificar se os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento.</p>	<p>Os controles de segurança normalmente não são tão rígidos no ambiente de desenvolvimento ou de teste. O uso dos dados de produção confere aos indivíduos mal-intencionados a oportunidade de obter acesso não autorizado aos dados de produção (dados do titular do cartão).</p>
<p><b>6.4.4</b> Exclusão dos dados de teste e contas dos componentes do sistema antes do sistema tornar-se ativo/entrar em produção.</p>	<p><b>6.4.4.a</b> Observe os processos de teste e questione os funcionários para verificar se os dados e as contas de teste são removidos antes que o sistema de produção se torne ativo.</p> <p><b>6.4.4.b</b> Analise uma amostra de dados e contas dos sistemas de produção recentemente instalados ou atualizados para verificar se estes são removidos antes que o sistema se torne ativo.</p>	<p>Dados e contas de teste devem ser removidos antes que o componente do sistema seja ativado (em produção), pois esses itens podem fornecer informações sobre o funcionamento do aplicativo ou do sistema. A posse dessas informações pode facilitar o comprometimento do sistema e dos dados relacionados ao titular do cartão.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.4.5</b> Mudanças nos procedimentos de controle devem incluir o seguinte:</p>	<p><b>6.4.5.a</b> Analise os procedimentos de controle de mudança documentados e verifique se os procedimentos estão definidos para:</p> <ul style="list-style-type: none"> <li>• Documentação de impacto</li> <li>• Aprovação documentada de alteração pelas partes autorizadas</li> <li>• Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema</li> <li>• Procedimentos de reversão</li> </ul> <p><b>6.4.5.b</b> Para obter uma amostra dos componentes do sistema, questione os funcionários responsáveis para determinar alterações recentes. Rastreie essas alterações com a documentação de controle de alteração relacionada. Para cada alteração analisada, desempenhe o seguinte:</p>	<p>Se não for adequadamente controlado, o impacto das mudanças no sistema - como atualizações de hardware ou software e instalação de patches de segurança - pode não ser realizado por completo e gerar consequências inesperadas.</p>
<p><b>6.4.5.1</b> Documentação de impacto.</p>	<p><b>6.4.5.1</b> Verifique se a documentação de impacto está incluída na documentação de controle de alterações para cada alteração exemplificada.</p>	<p>O impacto da alteração deve ser documentado de forma que todas as partes afetadas possam planejar adequadamente quaisquer alterações de processamento.</p>
<p><b>6.4.5.2</b> Aprovação documentada de alteração pelas partes autorizadas.</p>	<p><b>6.4.5.2</b> Verifique se a aprovação documentada por partes autorizadas está presente para cada alteração exemplificada.</p>	<p>A aprovação por partes autorizadas indica que a alteração é legítima e que a alteração aprovada foi sancionada pela organização.</p>
<p><b>6.4.5.3</b> Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema.</p>	<p><b>6.4.5.3.a</b> Para cada alteração exemplificada, verifique se o teste de funcionalidade foi realizado para verificar se a alteração não tem impacto adverso sobre a segurança do sistema.</p> <p><b>6.4.5.3.b</b> Para alterações de código personalizado, verifique se todas as atualizações foram testadas para estarem de acordo com o Requisito 6.5 do PCI DSS antes de serem implementadas na produção.</p>	<p>Deverão ser realizados testes rigorosos para verificar se a segurança do ambiente não se reduz ao ser implantada uma alteração. O teste deverá validar se todos os controles de segurança existentes permaneçam no lugar, sejam substituídos por controles igualmente rigorosos ou sejam reforçados após alguma alteração no ambiente.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
6.4.5.4 Procedimentos de reversão.	6.4.5.4 Verifique se os procedimentos de reversão foram preparados para cada alteração exemplificada.	Para cada alteração, deve haver procedimentos de reversão documentados para o caso de falhas na alteração ou efeitos adversos na segurança de um aplicativo ou sistema, a fim de permitir que o sistema seja restaurado ao seu estado anterior.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.4.6</b> Após concluir uma mudança significativa, todos os requisitos relevantes do PCI DSS devem ser implementados em todos os sistemas novos ou alterados e nas redes; a documentação deve ser atualizada, conforme aplicável.</p> <p><b>Observação:</b> <i>Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i></p>	<p><b>6.4.6</b> Para obter uma amostra das alterações significativas, analise os registros de mudança, converse com a equipe e observe os sistemas e redes afetadas para verificar se, como parte da mudança, os requisitos referente ao PCI DSS foram implementados e a documentação, atualizada.</p>	<p>Estabelecer processos para analisar mudanças significativas ajuda a garantir que todos os controles apropriados do PCI DSS serão aplicados para todas as redes ou sistemas adicionados ou alterados no ambiente do escopo.</p> <p>Estruturar a validação sobre processos de gestão de mudanças contribui para garantir que os padrões de configuração e inventários do dispositivo estejam sempre atualizados e os controles de segurança sejam aplicados onde necessário.</p> <p>O processo de gestão de mudanças deve incluir evidências capazes de comprovar que os requisitos do PCI DSS estejam implementados ou preservados através do processo iterativo.</p> <p>Exemplos de requisitos do PCI DSS que poderiam sofrer impacto incluem, entre outros:</p> <ul style="list-style-type: none"> <li>• Diagrama da rede atualizado para refletir as mudanças.</li> <li>• Sistemas configurados segundo os padrões de configuração, com todas as senhas padrão alteradas e serviços desnecessários desabilitados.</li> <li>• Sistemas protegidos com controles necessários — p. ex., monitoramento de integridade de arquivos (FIM), antivírus, patches e registro de auditoria.</li> <li>• Os dados de autenticação confidenciais (SAD) não são armazenados e todos os dados armazenados de titulares de cartão (CHD) são documentados e incorporados conforme os procedimentos e a política de retenção de dados</li> <li>• Novos sistemas são incluídos no processo trimestral de verificação de vulnerabilidade.</li> </ul>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.5</b> Trate as vulnerabilidades de codificação comuns nos processos de desenvolvimento do software conforme segue:</p> <ul style="list-style-type: none"> <li>• Ofereça treinamento aos desenvolvedores, pelo menos anualmente, transmitindo técnicas de codificação de segurança atualizadas, entre as quais, como evitar vulnerabilidades comuns de codificação.</li> <li>• Desenvolva aplicativos baseados nas diretrizes de código seguro.</li> </ul> <p><b>Observação:</b> as vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas de acordo com as práticas recomendadas pelo setor, quando esta versão do PCI DSS foi publicada. No entanto, conforme as práticas recomendadas pelo setor para o gerenciamento de vulnerabilidades são atualizadas (por exemplo o Guia OWASP, SANS CWE Top 25, CERT Secure Coding, etc.), as atuais práticas recomendadas devem ser usadas para estes requisitos.</p>	<p><b>6.5.a</b> Analise as políticas e os procedimentos de desenvolvimento de software para verificar se há exigência referente ao treinamento em técnicas de codificação seguras para desenvolvedores, pelo menos, anualmente, com base nas diretrizes e práticas recomendadas do setor.</p> <p><b>6.5.b</b> Consulte os registros de treinamento para verificar se os desenvolvedores de software receberam treinamento atualizado sobre técnicas seguras de codificação, pelo menos anualmente, inclusive sobre como evitar vulnerabilidades comuns de codificação.</p> <p><b>6.5.c</b> Verifique se há processos implementados para proteger os aplicativos contra, pelo menos, as seguintes vulnerabilidades:</p>	<p>A camada do aplicativo é de alto risco e pode ser tida como alvo por ameaças internas e externas.</p> <p>Os requisitos 6.5.1 a 6.5.10 são os controles mínimos que devem ser implementados e as organizações devem incorporar as práticas seguras de codificação relevantes conforme aplicável à tecnologia específica em seu ambiente.</p> <p>Os desenvolvedores de aplicativos devem ser treinados adequadamente para identificar e resolver problemas relacionados a estas (e outras) vulnerabilidades de codificação comuns. Uma equipe com conhecimento sobre as orientações seguras de codificação deve minimizar o número de vulnerabilidades de segurança introduzidas por meio de más práticas de codificação. O treinamento para os desenvolvedores pode ser ministrado no local ou por terceiros e deve ser aplicável à tecnologia utilizada.</p> <p>Todas as alterações de práticas de decodificação aceitas pelo setor, as práticas de decodificação organizacionais e o treinamento de desenvolvedores devem ser atualizados igualmente para lidar com novas ameaças, por exemplo, invasões relacionadas à limpeza de memória.</p> <p>As vulnerabilidades identificadas no 6.5.1 até o 6.5.10 oferecem uma linha de base mínima. É de escolha da organização permanecer atualizada com as tendências de vulnerabilidades e incorporar as medidas apropriadas em suas práticas seguras de codificação.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<b>Observação:</b> Os requisitos 6.5.1 a 6.5.6 abaixo se aplicam a todos os aplicativos (internos ou externos).		
<p><b>6.5.1</b> Falhas na injeção, particularmente na injeção SQL. também considere as falhas de injeção OS Command Injection, LDAP e XPath, assim como outras falhas.</p>	<p><b>6.5.1</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se as falhas de injeção são resolvidas pelas técnicas de codificação que incluem:</p> <ul style="list-style-type: none"> <li>• Validar a entrada para verificar se os dados do usuário não podem modificar o significado dos comandos e das consultas.</li> <li>• Utilizar consultas parametrizadas.</li> </ul>	<p>As falhas de injeção, principalmente de injeção de SQL, são um método comumente utilizado em aplicativos comprometidos. A injeção ocorre quando dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete para executar comandos não planejados ou para alterar os dados e permitem que o invasor invada os componentes dentro da rede por meio do aplicativo, a fim de iniciar invasões como sobrecargas do buffer, ou para revelar tanto informações confidenciais quando funcionalidades no aplicativo do servidor.</p> <p>As informações devem ser validadas antes de serem enviadas para o aplicativo, por exemplo, ao verificar todos os caracteres alfabéticos, mistura de caracteres alfabéticos e numéricos, etc.</p>
<p><b>6.5.2</b> Sobrecargas do buffer</p>	<p><b>6.5.2</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se as sobrecargas de buffer são resolvidas pelas técnicas de codificação que incluem:</p> <ul style="list-style-type: none"> <li>• Validar os limites do buffer.</li> <li>• Truncar as strings de entrada.</li> </ul>	<p>As sobrecargas de buffer ocorrem quando um aplicativo não possui uma verificação de limites adequada em seu espaço de buffer. Isto pode fazer com que as informações no buffer sejam empurradas para o espaço da memória do buffer e o espaço da memória executável. Quando isso ocorre, o invasor consegue inserir um código mal-intencionado no final do buffer e envie por push este código para o espaço de memória executável ao provocar sobrecarga de buffer. O código mal-intencionado é então executado e com frequência permite que o invasor acesse remotamente o aplicativo e/ou o sistema infectado.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.5.3</b> Armazenamento criptográfico não seguro</p>	<p><b>6.5.3</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se o armazenamento criptográfico não seguro é direcionado pelas técnicas de codificação que:</p> <ul style="list-style-type: none"> <li>• Evita falhas criptográficas.</li> <li>• Utiliza chaves e algoritmos de criptografia forte.</li> </ul>	<p>Os aplicativos que não utilizam recursos de criptografia robusta de forma adequada para armazenar dados correm um risco maior de comprometimento e exposição das credenciais de autenticação e/ou dados do titular do cartão. Caso um invasor consiga explorar os processos criptográficos, ele poderá obter acesso de texto simples aos dados criptografados.</p>
<p><b>6.5.4</b> Comunicações não seguras</p>	<p><b>6.5.4</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se as comunicações não seguras são direcionadas pelas técnicas de codificação que autenticam e criptografam corretamente todas as comunicações confidenciais.</p>	<p>Os aplicativos que não criptografarem adequadamente o tráfego de rede utilizando criptografia robusta correm um risco maior de comprometimento e exposição dos dados do titular do cartão. Se conseguir explorar os processos criptografados, o invasor poderá obter controle sobre um aplicativo ou, até mesmo, obter acesso em texto simples a dados criptografados.</p>
<p><b>6.5.5</b> Tratamento incorreto de erros</p>	<p><b>6.5.5</b> Analise as políticas e procedimentos de desenvolvimento de software e converse com os funcionários responsáveis para verificar se o tratamento incorreto de erros é direcionado pelas técnicas de codificação que não vazam informações por meio de mensagens de erro (por exemplo, retornando detalhes de erros genéricos em vez de erros específicos).</p>	<p>Os aplicativos podem, de forma não intencional, vazam informações sobre sua configuração, trabalhos internos ou expor informações privilegiadas por meio de métodos de tratamento de erros. Os invasores usam esse ponto fraco para roubar dados confidenciais ou para comprometer o sistema como um todo. Se um indivíduo mal-intencionado puder criar erros que o aplicativo não consegue manusear corretamente, eles podem obter informações detalhadas do sistema, criar interrupções de negação de serviço, causar falhas de segurança ou criar problemas no servidor. Por exemplo, a mensagem “senha incorreta” informa ao invasor que o ID de usuário fornecido está correto e que ele deve concentrar os esforços somente na senha. Use mensagens de erro mais genéricas, como “os dados não puderam ser verificados”.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.5.6</b> Todas as vulnerabilidades de “alto risco” identificadas no processo de identificação de vulnerabilidade (conforme definido no Requisito 6.1 do PCI DSS).</p>	<p><b>6.5.6</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se as técnicas de codificação resolvem qualquer vulnerabilidade de “alto risco” que possa afetar o aplicativo, conforme identificado no Requisito 6.1 do PCI DSS.</p>	<p>Todas as vulnerabilidades identificadas pelo processo de classificação de risco de vulnerabilidade de uma organização (definido no Requisito 6.1) como sendo de “alto risco” e que possam afetar o aplicativo devem ser identificadas e resolvidas durante o desenvolvimento do aplicativo.</p>
<p><b>Observação:</b> Os Requisitos 6.5.7 a 6.5.10 abaixo se aplicam a aplicativos da Web e em interfaces de aplicativos (internos ou externos):</p>		<p>Os aplicativos da Web, tanto internos quanto externos (públicos), possuem riscos de segurança exclusivos com base em sua arquitetura e sua relativa facilidade em apresentar comprometimento.</p>
<p><b>6.5.7</b> Script intersite (XSS)</p>	<p><b>6.5.7</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se o script intersite (XSS) é direcionado pelas técnicas de codificação que incluem</p> <ul style="list-style-type: none"> <li>• Validar todos os parâmetros antes da inclusão</li> <li>• Utilizar saída de contexto confidencial.</li> </ul>	<p>Ocorrem falhas no XSS sempre que o aplicativo coletar os dados fornecidos pelo usuário e enviá-los para um navegador sem primeiro validar ou codificar esse conteúdo. O XSS permite que os invasores executem o script no navegador da vítima, que pode se apoderar de sessões de usuários, desfigurar sites, possivelmente introduzir worms, etc.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.5.8</b> Controle de acesso inadequado (como referências diretas não seguras a objetos, falhas em restringir o acesso a URLs, diretórios transversais e falhas em restringir o acesso do usuário às funções).</p>	<p><b>6.5.8</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se o controle de acesso incorreto (como referências diretas não seguras a objetos, falha em restringir o acesso a URLs e diretórios transversais) é direcionado pelas técnicas de codificação que incluem:</p> <ul style="list-style-type: none"> <li>• Autenticação adequada dos usuários</li> <li>• Limpar a entrada</li> <li>• Não expor referências de objetos internos aos usuários</li> <li>• As interfaces do usuário não permitem o acesso a funções não autorizadas.</li> </ul>	<p>Uma referência de objeto direto ocorre quando o desenvolvedor expõe uma referência a um objeto de implementação interna, como arquivo, diretório, registro de banco de dados ou chave, como um URL ou forma de parâmetro. Os invasores podem manipular essas referências para acessar outros objetos sem autorização.</p> <p>Force constantemente o controle de acesso na camada de apresentação e na lógica de negócios para todos os URLs. Muitas vezes um aplicativo só protege os recursos confidenciais ao evitar a exibição de links ou URLs para usuários não autorizados. Os invasores podem usar esse ponto fraco para acessar e executar operações não autorizadas, acessando diretamente esses URLs.</p> <p>Um invasor poderá ser capaz de enumerar e navegar pela estrutura do diretório de um site (diretório transversal), obtendo acesso a informações não autorizadas e descobrindo o funcionamento do site para exploração futura.</p> <p>Se as interfaces do usuário permitirem acesso a funções não autorizadas, o acesso concedido pode fazer com que indivíduos não autorizados obtenham acesso a credenciais privilegiadas ou aos dados do titular do cartão. Apenas usuários autorizados devem ter permissão para acessar as referências diretas de objetos a recursos confidenciais. Limitar o acesso aos recursos de dados ajudará a evitar que os dados do titular do cartão sejam apresentados a recursos não autorizados.</p>
<p><b>6.5.9</b> Solicitação intersite forjada (CSRF).</p>	<p><b>6.5.9</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se a solicitação intersite forjada (CSRF) é direcionada pelas técnicas de codificação que garantem que os aplicativos não contem com tokens e credenciais de autorização automaticamente enviados pelos navegadores.</p>	<p>Um invasão de CSRF força o navegador da vítima logada a enviar uma solicitação pré-autenticada a um aplicativo da Web vulnerável, que então possibilita ao invasor realizar qualquer operação de modificação do status que a vítima tenha autorização para realizar (como atualizar detalhes da conta, fazer aquisições ou até mesmo autenticar ao aplicativo).</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.5.10</b> Autenticação quebrada e gerenciamento de sessão</p>	<p><b>6.5.10</b> Analise as políticas e procedimentos de desenvolvimento de software e questione os funcionários responsáveis para verificar se a autenticação quebrada e o gerenciamento de sessão são resolvidos pelas técnicas de codificação que comumente incluem:</p> <ul style="list-style-type: none"> <li>• Marcar os tokens de sessão (por exemplo, cookies) como "seguro"</li> <li>• Não expor os IDs de sessão no URL</li> <li>• Incorporar períodos de tempo apropriados e rotação de IDs de sessão depois de efetuar logon com sucesso.</li> </ul>	<p>A autenticação segura e gerenciamento de sessão evita que indivíduos não autorizados comprometam as credenciais, chaves ou tokens de sessão legítimos da conta, o que pode permitir que o invasor assuma a identidade de um usuário autorizado.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.6</b> Para aplicativos da Web voltados ao público, trate novas ameaças e vulnerabilidades continuamente e assegure que esses aplicativos estejam protegidos contra invasões conhecidos por meio de qualquer um dos métodos a seguir:</p> <ul style="list-style-type: none"> <li>• Analisar os aplicativos da Web voltados ao público por meio de ferramentas ou métodos manuais ou automáticos de avaliação de segurança das vulnerabilidades dos aplicativos, pelo menos anualmente e após quaisquer alterações</li> </ul> <p><b>Observação:</b> <i>esta avaliação não é igual às varreduras de vulnerabilidades realizadas para o Requisito 11.2.</i></p> <ul style="list-style-type: none"> <li>• Instalar uma solução técnica automatizada que detecte e previna invasões baseadas na Web (por exemplo, um firewall de aplicativo na Web) na frente de aplicativos da Web voltados para o público, para verificar continuamente todo o tráfego.</li> </ul>	<p><b>6.6</b> Para <i>aplicativos da Web</i> voltados ao público, certifique-se de que <i>qualquer um</i> dos métodos a seguir esteja implementado conforme se segue:</p> <ul style="list-style-type: none"> <li>• Analise os processos documentados, questione os funcionários e analise os registros de avaliação de segurança do aplicativo para verificar se os aplicativos da Web voltados ao público são analisados (usando ferramentas ou métodos manuais ou automatizados de avaliação de segurança das vulnerabilidades) conforme segue: <ul style="list-style-type: none"> <li>– Pelo menos uma vez ao ano</li> <li>– Após quaisquer alterações</li> <li>– Por meio de uma empresa especializada na segurança de aplicativos</li> <li>– Se, pelo menos, todas as vulnerabilidades no Requisito 6.5 estão incluídas na avaliação</li> <li>– Se todas as vulnerabilidades são corrigidas</li> <li>– Se o aplicativo é reavaliado após as correções.</li> </ul> </li> <li>• Analise os ajustes da configuração do sistema e questione os funcionários para verificar se uma solução técnica automatizada que detecte e previna invasões baseadas na Web (por exemplo, um firewall de aplicativo na Web) seja implementada conforme segue: <ul style="list-style-type: none"> <li>– Está situada diante de aplicativos da web voltados ao público para detectar e prevenir invasões baseadas na web.</li> <li>– Está funcionando ativamente e atualizada conforme aplicável.</li> <li>– Está gerando logs de auditoria.</li> <li>– Está configurado para bloquear ataques baseados na web, ou gerar um alerta que é imediatamente investigado.</li> </ul> </li> </ul>	<p>Os aplicativos da Web voltados ao público são alvos principais de invasores e se não estiverem bem codificados, proporcionam caminho fácil para que os invasores obtenham acesso aos dados e sistemas confidenciais. O requisito para analisar aplicativos ou instalar firewalls de aplicativos da Web destina-se a reduzir o número de comprometimentos em aplicativos da Web devido à má codificação ou más práticas de gerenciamento do aplicativo.</p> <ul style="list-style-type: none"> <li>• Ferramentas ou métodos de avaliação da segurança de vulnerabilidade manual ou automatizada analisam e/ou testam o aplicativo para identificar vulnerabilidades</li> <li>• Firewalls de aplicativo da Web filtram e bloqueiam tráfego não essencial na camada do aplicativo. Utilizado em conjunto com um firewall com base em rede, um firewall de aplicativo da Web configurado corretamente evita invasões na camada de aplicativos caso estes estejam codificados ou configurados incorretamente. Isto pode ser conseguido pela combinação entre tecnologia e processo. Soluções baseadas em processos devem oferecer mecanismos que facilitam respostas aos alertas em tempo hábil para atender ao objetivo deste requisito; qual seja, evitar ataques.</li> </ul> <p><b>Observação:</b> <i>“Uma empresa especializada na segurança de aplicativos” pode ser uma empresa terceirizada ou uma empresa interna, desde que os analisadores sejam especializados na segurança de aplicativos e possam demonstrar que não dependem da equipe de desenvolvimento.</i></p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>6.7</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para desenvolver e manter os sistemas e aplicativos estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>6.7</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e procedimentos operacionais para desenvolver e manter os sistemas e aplicativos estão:</p> <ul style="list-style-type: none"><li>• Documentados,</li><li>• Em uso, e</li><li>• Conhecidos por todas as partes envolvidas.</li></ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para garantir que os sistemas e aplicativos sejam desenvolvidos com segurança e continuamente protegidos contra vulnerabilidades.</p>

## Implementar medidas rigorosas de controle de acesso

### **Requisito 7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio**

Para assegurar que os dados críticos possam ser acessados somente por uma equipe autorizada, os sistemas e processos devem estar implementados para limitar o acesso com base na necessidade de divulgação e de acordo com as responsabilidades da função.

A “necessidade de divulgação” é quando os direitos de acesso são concedidos somente ao menor número possível de dados e privilégios necessários para realizar um trabalho.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>7.1</b> Limite o acesso aos componentes do sistema e aos dados do titular do cartão somente àquelas pessoas cuja função requer tal acesso.</p>	<p><b>7.1</b> Analise a política por escrito para o controle de acesso e verifique se a política incorpora os requisitos 7.1.1 a 7.1.4 conforme segue:</p> <ul style="list-style-type: none"> <li>Definir necessidades de acesso e atribuições especiais para cada função</li> <li>Restrição de acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função</li> <li>A concessão do acesso se baseia na classificação e na atribuição da função da equipe individual</li> <li>Aprovação documentada (eletronicamente ou por escrito) pelas partes autorizadas a todo o acesso, incluindo lista de privilégios específicos aprovados.</li> </ul>	<p>Quanto mais pessoas tiverem acesso aos dados do titular do cartão, mais risco haverá de que a conta do usuário seja utilizada indevidamente. Limitar o acesso a pessoas com motivo corporativo legítimo para o acesso ajuda a organização a evitar o uso indevido dos dados do titular do cartão, em razão de inexperiência ou má intenção.</p>
<p><b>7.1.1</b> Defina as necessidades de acesso para cada função, incluindo:</p> <ul style="list-style-type: none"> <li>Componentes do sistema e recursos de dados que cada função precisa acessar para realizar seu trabalho</li> <li>O nível de privilégio necessário (por exemplo, usuário, administrador, etc.) para acessar os recursos.</li> </ul>	<p><b>7.1.1</b> Selecione uma amostra de funções e verifique se as necessidades de acesso para cada função estão definidas e se incluem:</p> <ul style="list-style-type: none"> <li>Componentes do sistema e recursos de dados que cada função precisa acessar para realizar seu trabalho</li> <li>Identificação do privilégio necessário para cada função realizar seu trabalho.</li> </ul>	<p>Para limitar o acesso aos dados do titular do cartão somente aos indivíduos que precisam do acesso, primeiramente, é preciso definir as necessidades de acesso para cada função (por exemplo, administrador do sistema, equipe da central de atendimento, balconista), os sistemas/dispositivos/dados que cada função precisa acessar e o nível de privilégio que cada função precisa para desempenhar efetivamente as tarefas atribuídas. Uma vez que as funções e necessidades de acesso correspondentes estiverem definidas, os indivíduos terão o direito de acesso. <i>(Continua na próxima página)</i></p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>7.1.2</b> Restrinja o acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função.</p>	<p><b>7.1.2.a</b> Converse com os funcionários responsáveis por permitir o acesso para verificar se o acesso a IDs de usuários privilegiados é:</p> <ul style="list-style-type: none"> <li>• Permitido apenas às funções que requerem especificamente tal acesso privilegiado</li> <li>• Restritos ao menor número de privilégios necessários para o desempenho das responsabilidades da função.</li> </ul>	<p>Ao atribuir IDs privilegiados, é importante atribuir aos indivíduos apenas os privilégios que eles precisam para desempenhar seu trabalho (o "mínimo de privilégios"). Por exemplo, o administrador do bando de dados ou do backup não deve ter os mesmos privilégios que o administrador dos sistemas como um todo.</p>
	<p><b>7.1.2.b</b> Selecione uma amostra de IDs de usuário com acesso privilegiado e questione a equipe de gerenciamento responsável para verificar se os privilégios concedidos são:</p> <ul style="list-style-type: none"> <li>• Necessários para a função daquela pessoa</li> <li>• Restritos ao menor número de privilégios necessários para o desempenho das responsabilidades da função.</li> </ul>	<p>Conceder o mínimo de privilégios ajuda a evitar que usuários sem conhecimento suficiente sobre o aplicativo alterem incorretamente ou acidentalmente a configuração do aplicativo ou alterem seus ajustes de segurança. Executar o mínimo de privilégios também ajuda a minimizar os danos de uma pessoa não autorizada obter acesso ao ID do usuário.</p>
<p><b>7.1.3</b> Conceda acesso com base na classificação e na atribuição da função de cada indivíduo da equipe.</p>	<p><b>7.1.3</b> Selecione uma amostra de IDs de usuário e questione a equipe de gerenciamento responsável para verificar se os privilégios concedidos baseiam-se na classificação e atribuição da função do indivíduo.</p>	<p>Quando as necessidades estiverem definidas para as funções do usuário (conforme o requisito 7.1.1 do PCI DSS), é fácil conceder o acesso aos indivíduos de acordo com sua função e classificação de seu trabalho utilizando as funções já criadas.</p>
<p><b>7.1.4</b> Solicite aprovação documentada por partes autorizadas especificando os privilégios exigidos.</p>	<p><b>7.1.4</b> Selecione uma amostra dos IDs de usuário e compare com as aprovações documentadas para verificar se:</p> <ul style="list-style-type: none"> <li>• Existe aprovação documentada para os privilégios atribuídos</li> <li>• A aprovação foi realizada pelas partes autorizadas</li> <li>• Os privilégios especificados correspondem com as funções atribuídas ao indivíduo.</li> </ul>	<p>A aprovação documentada (por exemplo, por escrito ou eletronicamente) garante que as pessoas com acesso e privilégios estejam cientes e autorizadas pelo gerenciamento e que seu acesso seja necessário para suas funções.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>7.2</b> Estabeleça sistema(s) de controle de acesso para os componentes do sistemas que limitem o acesso com base na necessidade de conhecimento do usuário e que estejam configurados para “recusar todos”, salvo se houver permissão específica.</p> <p>O(s) sistema(s) de controle de acesso deve(m) incluir o seguinte:</p>	<p><b>7.2</b> Analise as configurações do sistema e a documentação do fornecedor para verificar se o(s) sistema(s) de controle de acesso está(ão) implementado(s), conforme a seguir:</p>	<p>Sem um mecanismo para restringir acesso com base na necessidade de conhecimento, o usuário pode receber acesso aos dados do titular do cartão equivocadamente. Os sistemas de controle de acesso automatizam o processo de restrição de acesso e atribuição de privilégios. Além disso, uma configuração padrão “recusar todos” garante que ninguém tenha acesso até ou a menos que uma regra seja estabelecida especificamente concedendo este acesso. As entidades podem ter um ou mais sistemas de controles de acesso para gerenciar o acesso do usuário.</p>
<p><b>7.2.1</b> Abrangência de todos os componentes do sistema</p>	<p><b>7.2.1</b> Confirme se os sistemas de controle de acesso foram implementados em todos os componentes do sistema.</p>	
<p><b>7.2.2</b> A concessão dos privilégios aos indivíduos está baseada na classificação e na atribuição da função.</p>	<p><b>7.2.2</b> Confirme se os sistemas de controle de acesso estão configurados para impor os privilégios concedidos às pessoas com base na classificação e na atribuição da função.</p>	<p><b>Observação:</b> Alguns sistemas de controle de acesso são definidos, como padrão, como “permitir todos”, permitindo, portanto, o acesso a menos que/até que uma norma seja redigida para recusá-lo de forma específica.</p>
<p><b>7.2.3</b> Configuração padrão “recusar todos”.</p>	<p><b>7.2.3</b> Confirme se os sistemas de controle de acesso têm uma configuração padrão “recusar todos”.</p>	
<p><b>7.3</b> Certifique-se de que as políticas de segurança e os procedimentos operacionais para restringir o acesso aos dados do titular do cartão estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>7.3</b> Analise a documentação e converse com os funcionários para verificar se as políticas de segurança e os procedimentos operacionais para restringir o acesso aos dados do titular do cartão estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para garantir que o acesso seja continuamente controlado e com base na necessidade de conhecimento e no mínimo de privilégios.</p>

## Requisito 8: **Identifique e autentique o acesso aos componentes do sistema**

Atribuir uma identificação exclusiva (ID) a cada pessoa com acesso assegura que cada indivíduo seja exclusivamente responsável pelas suas ações. Quando tal responsabilidade estiver em vigor, as ações desempenhadas nos dados e sistemas críticos serão realizadas e podem ser rastreadas, por usuários e processos conhecidos e autorizados.

A efetividade de uma senha é largamente determinada pelo projeto e implementação do sistema de autenticação, particularmente, com que frequência um invasor pode fazer tentativas de senha e os métodos de segurança para proteger as senhas do usuário no ponto de entrada, durante a transmissão e enquanto estiver armazenada.

**Observação:** *Esses requisitos aplicam-se a todas as contas, inclusive contas de pontos de venda com capacidades administrativas e todas as contas usadas para visualizar ou acessar os dados do titular do cartão ou acessar sistemas com dados do titular do cartão. Isso inclui as contas usadas por fornecedores e outros terceiros (por exemplo, para suporte e manutenção). Estes requisitos não se aplicam a contas usadas por consumidores (p. ex., titulares de cartões).*

*No entanto, os requisitos 8.1.1, 8.2, 8.5, 8.2.3 até o 8.2.5 e o 8.1.6 até o 8.1.8 não têm por objetivo serem aplicados a contas de usuário em um aplicativo de pagamento de um ponto de venda que possua acesso somente a um número de cartão por vez para facilitar a transação única (como contas de caixa).*

Requisitos do PCI DSS	Procedimentos de teste	Orientação
8.1 Defina e implemente políticas e procedimentos para garantir o gerenciamento adequado da identificação do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, conforme segue:	8.1.a Revise os procedimentos e confirme se eles definem processos para cada um dos itens abaixo em 8.1.1 até 8.1.8	Ao garantir que todos os usuários sejam individualmente identificados, em vez de usar um ID para vários funcionários, uma organização consegue manter a responsabilidade individual pelas ações e uma trilha de auditoria eficaz por funcionário. Isso ajudará a apressar a resolução e a contenção de problemas quando ocorrer mau uso ou tentativa mal-intencionada.
	8.1.b Verifique se os processos foram implementados para o gerenciamento de identificação do usuário, realizando o seguinte:	
8.1.1 Atribua a todos os usuários uma identificação exclusiva antes de permitir acesso aos componentes do sistema ou aos dados do titular do cartão.	8.1.1 Converse com a equipe administrativa para confirmar se todos os usuários receberam uma identidade exclusiva para acesso aos componentes do sistema ou aos dados do titular do cartão.	
8.1.2 Controle o acréscimo, a exclusão e a modificação dos IDs do usuário, credenciais e outros objetos do responsável pela identificação.	8.1.2 Para obter uma amostra dos IDs de usuários privilegiados e IDs de usuários gerais, analise as autorizações associadas e observe os ajustes do sistema para verificar se cada ID do usuário e ID do usuário privilegiado foi implementado apenas com os privilégios especificados na aprovação documentada.	Para garantir que as contas de usuário com acesso aos sistemas são todas usuários válidos e reconhecidos, processos rigorosos devem controlar todas as modificações nos IDs de usuário e outras credenciais de autenticação, incluindo adicionar novos e modificar ou excluir os existentes.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.1.3</b> Revogue imediatamente o acesso de quaisquer usuários desligados da empresa.</p>	<p><b>8.1.3.a</b> Selecione uma amostra de funcionários desligados da empresa nos últimos seis meses e analise as listas de acesso dos usuários atuais, tanto para o acesso remoto quanto o local, a fim de verificar se seus IDs foram desativados ou removidos das listas de acesso.</p> <p><b>8.1.3.b</b> Verifique se todos os métodos físicos de autenticação (como smart cards, tokens, etc.) tenham sido devolvidos ou desativados.</p>	<p>Se ao deixar a empresa o funcionário ainda tiver acesso à rede por meio da conta de usuário, a empresa estará sujeita ao acesso indevido ou mal-intencionado aos dados do titular do cartão — pelo antigo funcionário ou por um usuário mal-intencionado que se aproveite da conta antiga e/ou não utilizada. Para prevenir o acesso não autorizado, as credenciais do usuário e outros métodos de autenticação precisam ser revogados imediatamente (assim que possível) à saída do funcionário.</p>
<p><b>8.1.4</b> Remover/desativar contas inativas do usuário no prazo de 90 dias.</p>	<p><b>8.1.4</b> Observe as contas do usuário para verificar se as contas inativas por mais de 90 dias são removidas ou desativadas.</p>	<p>As contas não usadas regularmente são alvos frequentes de invasões, pois é menos provável que qualquer alteração (como uma senha alterada) seja notada. Desse modo, estas contas podem ser exploradas mais facilmente e usadas para acessar os dados do titular do cartão.</p>
<p><b>8.1.5</b> Controle as IDs usadas por terceiros para acessar, dar suporte ou manter os componentes do sistema via acesso remoto, conforme segue:</p> <ul style="list-style-type: none"> <li>• Ativar apenas durante o período necessário e desativar quando não estiverem em uso.</li> <li>• Monitorar quando estiverem em uso.</li> </ul>	<p><b>8.1.5.a</b> Converse com os funcionários e observe os processos para gerenciar contas usadas por terceiros para acessar, dar suporte ou manter os componentes do sistema, com a finalidade de verificar se as contas usadas para acesso remoto são:</p> <ul style="list-style-type: none"> <li>• Desativadas quando não estão em uso</li> <li>• Ativadas por terceiros apenas quando necessário e desativadas quando não estão em uso.</li> </ul> <p><b>8.1.5.b</b> Converse com os funcionários e observe os processos para verificar se as contas de acesso remoto usadas por terceiros são monitoradas quando em uso.</p>	<p>Permitir que fornecedores tenham acesso integral à sua rede caso eles precisem dar suporte ao seu sistema aumenta as chances de acesso não autorizado, seja de um usuário no ambiente do fornecedor ou de um indivíduo mal-intencionado que descubra e use esse ponto de entrada externo sempre pronto para sua rede. Ativar o acesso apenas pelos períodos de tempo necessários e desativar assim que não for mais necessário, ajuda a prevenir o mau uso destas conexões.</p> <p>O monitoramento do acesso do fornecedor proporciona a garantia de que os fornecedores estejam acessando apenas os sistemas necessários e somente durante os períodos de tempo aprovados.</p>
<p><b>8.1.6</b> Limite tentativas de acesso repetidas bloqueando o ID do usuário após seis tentativas, no máximo.</p>	<p><b>8.1.6.a</b> Para obter uma amostra dos componentes do sistema, inspecione as configurações do sistema para verificar se os parâmetros de autenticação estão definidos para exigir que as contas de usuários sejam bloqueadas após seis tentativas inválidas de efetuar login.</p>	<p>Sem a implementação de mecanismos de bloqueio de conta, um invasor pode tentar continuamente adivinhar uma senha por meio de ferramentas manuais ou automatizadas (por exemplo, cracking de senha) até ter sucesso e ganhar acesso à conta</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>8.1.6.b Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Analise os processos internos e a documentação do cliente/usuário e observe os processos implementados para verificar se as contas do usuário que não é cliente são bloqueadas temporariamente após, no máximo, seis tentativas inválidas de acesso.</p>	<p>do usuário.</p> <p><b>Observação:</b> O procedimento de teste 8.1.6.b é um procedimento adicional que se aplica somente quando a entidade a ser avaliada tratar-se de um prestador de serviços.</p>
<p><b>8.1.7</b> Defina a duração do bloqueio para um mínimo de 30 minutos ou até que o administrador ative o ID do usuário.</p>	<p><b>8.1.7</b> Para obter uma amostra dos componentes do sistema, analise as configurações do sistema para verificar se os parâmetros de senha estão definidos para exigir que assim que a conta de um usuário for bloqueada, ela permanecerá dessa forma por pelo menos 30 minutos ou até que um administrador do sistema reconfigure a conta.</p>	<p>Se uma conta estiver bloqueada em função de uma pessoa tentar continuamente adivinhar a senha, os controles para atrasar a reativação dessas contas bloqueadas evitarão que o indivíduo mal-intencionado continue a tentar adivinhar a senha (ele terá de parar por pelo menos 30 minutos até a conta ser reativada). Além disso, se a reativação precisar ser solicitada, a administração ou o serviço de suporte pode validar se é o real proprietário da conta que está solicitando a reativação.</p>
<p><b>8.1.8</b> Se uma sessão estiver ociosa por mais de 15 minutos, solicite que o usuário redigite a senha para reativar o terminal.</p>	<p><b>8.1.8</b> Para obter uma amostra dos componentes do sistema, analise as definições de configuração do sistema para verificar se os recursos de tempo esgotado de ociosidade do sistema/sessão foram definidos para 15 minutos ou menos.</p>	<p>Quando os usuários se distanciam de uma máquina aberta com acesso a componentes críticos do sistema ou dados do titular do cartão, a máquina poderá ser usada por outras pessoas na ausência do usuário, resultando em acesso não autorizado e/ou uso indevido da conta.</p> <p>A reautenticação pode ser aplicada no nível de sistema para proteger todas as sessões em funcionamento naquela máquina, ou no nível de aplicativo.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.2</b> Além de atribuir uma ID exclusiva, garanta que um controle adequado da autenticação do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, empregando pelo menos um dos métodos a seguir para autenticar todos os usuários:</p> <ul style="list-style-type: none"> <li>• Algo que você sabe, como uma senha ou frase de senha</li> <li>• Algo que você tem, como um dispositivo de token ou um smart card</li> <li>• Algo que você é, como a biométrica.</li> </ul>	<p><b>8.2</b> Para verificar se os usuários são autenticados usando a identificação exclusiva e a autenticação adicional (por exemplo, uma senha/frase-senha) para acessar o ambiente de dados do titular do cartão, execute as medidas a seguir:</p> <ul style="list-style-type: none"> <li>• Analise a documentação que descreve o(s) método(s) de autenticação usado(s).</li> <li>• Para cada tipo do método de autenticação usado e para cada tipo do componente de sistema, observe uma autenticação para verificar se a autenticação está sendo executada de acordo com o(s) método(s) de autenticação documentado(s).</li> </ul>	<p>Esses métodos de autenticação, quando usados além dos IDs exclusivos, ajudam a proteger os IDs dos usuários contra o comprometimento, visto que quem estiver tentando as necessidades de comprometimento precisa conhecer tanto o ID exclusivo quanto a senha (ou outro item de autenticação). Observe que um certificado digital é uma opção válida para “algo que você tem” desde que seja exclusivo.</p> <p>Como uma das primeiras etapas tomadas por um indivíduo mal-intencionado para comprometer um sistema é explorar senhas fracas ou inexistentes, é importante implementar bons processos para controle de autenticação.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.2.1</b> Use criptografia forte, converta todas as credenciais de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema.</p>	<p><b>8.2.1.a</b> Analise a documentação do fornecedor e os ajustes da configuração do sistema para verificar se as senhas estão protegidas com criptografia forte durante a transmissão e o armazenamento.</p>	<p>Muitos dispositivos de rede e aplicativos transmitem senhas sem criptografia e legíveis por uma rede e/ou armazenam as senhas sem criptografia. Um indivíduo mal-intencionado pode facilmente interceptar as senhas sem criptografia durante a transmissão usando um “sniffer”, ou então acessar diretamente as senhas não criptografadas em arquivos onde eles são armazenados e usar esses dados para obter acesso não autorizado.</p> <p><b>Observação:</b> Os procedimentos de teste 8.2.1.d e 8.2.1.e são procedimentos adicionais que se aplicam somente quando a entidade a ser avaliada é um prestador de serviços.</p>
	<p><b>8.2.1.b</b> Para obter uma amostra dos componentes do sistema, analise os arquivos de senha para verificar se as senhas estão ilegíveis durante o armazenamento.</p>	
	<p><b>8.2.1.c</b> Para obter uma amostra dos componentes do sistema, analise as transmissões de dados para verificar se as senhas estão ilegíveis durante a transmissão.</p>	
	<p><b>8.2.1.d Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Observe os arquivos de senha para verificar se as senhas do usuário não-cliente estão ilegíveis durante o armazenamento.</p>	
	<p><b>8.2.1.e Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Observe as transmissões de dados para verificar se as senhas do usuário não-cliente estão ilegíveis durante a transmissão.</p>	
<p><b>8.2.2</b> Verifique a identidade do usuário antes de modificar qualquer credencial de autenticação, por exemplo, executar restauração da senha, provisionar novos tokens ou gerar novas chaves.</p>	<p><b>8.2.2</b> Analise os procedimentos de autenticação para modificar as credenciais de autenticação e observe a equipe de segurança para verificar se, caso um usuário solicite uma redefinição credencial de autenticação por telefone, e-mail, Web ou outro método remoto, a identidade do usuário é comprovada antes que a credencial de autenticação seja modificada.</p>	<p>Muitos indivíduos mal-intencionados usam a “engenharia social” (por exemplo, ligam para o serviço de suporte e agem como um usuário legítimo) para trocar a senha, de forma que possam utilizar um ID de usuário. Considere usar uma “pergunta secreta” que só o próprio usuário possa responder para ajudar os administradores a identificar o usuário antes de redefinir ou modificar as credenciais de autenticação.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.2.3</b> As senhas/frases-senha devem atender ao seguinte:</p> <ul style="list-style-type: none"> <li>• Exigir uma extensão mínima de pelo menos sete caracteres.</li> <li>• Conter caracteres numéricos e alfabéticos.</li> </ul> <p>Alternativamente, as senhas/frases-senha devem ter complexidade e força, pelo menos, equivalentes aos parâmetros especificados acima.</p>	<p><b>8.2.3a</b> Para obter uma amostra dos componentes do sistema, analise as definições de configuração do sistema para verificar se os parâmetros de senha/frase-senha do usuário estão definidos para solicitar, pelo menos, a seguinte complexidade/força:</p> <ul style="list-style-type: none"> <li>• Exigir uma extensão mínima de pelo menos sete caracteres.</li> <li>• Conter caracteres numéricos e alfabéticos.</li> </ul> <p><b>8.2.3.b Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Analise os processos internos e a documentação do cliente/usuário para verificar se as senhas/frases-senha do usuário não-cliente são exigidas para atender, pelo menos, a seguinte complexidade/força:</p> <ul style="list-style-type: none"> <li>• Exigir uma extensão mínima de pelo menos sete caracteres.</li> <li>• Conter caracteres numéricos e alfabéticos.</li> </ul>	<p>Senhas/frases-senha robustas são a primeira linha de defesa para rede, pois um indivíduo mal-intencionado, muitas vezes, tentará primeiro encontrar contas com senhas fracas ou inexistentes. Se as senhas forem curtas ou fáceis de adivinhar, é relativamente fácil para um indivíduo mal-intencionado localizar essas contas fracas e comprometer uma rede parecendo um ID de usuário válido.</p> <p>Este requisito especifica que, no mínimo, sete caracteres numéricos e alfabéticos devem ser usados para senhas/frases-senha. Para os casos em que este mínimo não é possível devido a limitações técnicas, as entidades podem usar “força equivalente” para avaliar sua alternativa. Para obter informações sobre a variabilidade e a equivalência da potência (também referida como entropia) para senhas/frases-senha de diferentes formatos, consulte as normas do setor (p. ex., a versão atualizada do NIST SP 800-63).</p> <p><b>Observação:</b> O procedimento de teste 8.2.3.b é um procedimento adicional que se aplica somente quando a entidade a ser avaliada tratar-se de um prestador de serviços.</p>
<p><b>8.2.4</b> Altere as senhas/frases-senha do usuário, pelo menos, a cada 90 dias.</p>	<p><b>8.2.4.a</b> Para obter uma amostra dos componentes do sistema, analise as definições de configuração do sistema para verificar se os parâmetros de senha/frases-senha do usuário estão definidos para solicitar que os usuários alterem as senhas, pelo menos, a cada 90 dias.</p> <p><b>8.2.4.b Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Revise os processos internos e a documentação do cliente/usuário para verificar se:</p> <ul style="list-style-type: none"> <li>• As senhas/frases-senha dos usuários não-clientes devem ser alteradas periodicamente; e</li> <li>• Usuários que não são clientes recebem instruções sobre quando e sob quais circunstâncias as senhas/frases-senha devem ser alteradas.</li> </ul>	<p>As senhas/frases-senha válidas por muito tempo e sem alteração proporcionam mais tempo a indivíduos mal-intencionados para tentativas de burlar a senha/frase-senha.</p> <p><b>Observação:</b> O procedimento de teste 8.2.4.b é um procedimento adicional que se aplica somente quando a entidade a ser avaliada tratar-se de um prestador de serviços.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.2.5</b> Não permita que ninguém envie uma nova senha/frase-senha que seja igual a uma das quatro últimas senhas/frases-senha usadas.</p>	<p><b>8.2.5.a</b> Para obter uma amostra dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha estão definidos para solicitar que as novas senhas/frases-senha não possam ser iguais às quatro senhas usadas anteriormente.</p> <p><b>8.2.5.b Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Analise os processos internos e a documentação do cliente/usuário para certificar-se de que as novas senhas/frases-senha do usuário não-cliente não poderão ser iguais às quatro senhas anteriores.</p>	<p>Se o histórico da senha não for mantido, a efetividade da alteração da senha é reduzida, já que as senhas anteriores podem ser reutilizadas várias vezes. Determinar que as senhas não sejam reutilizadas por um período de tempo reduz a probabilidade de que senhas que foram adivinhadas ou violadas sejam usadas futuramente.</p> <p><b>Observação:</b> O procedimento de teste 8.2.5.b é um procedimento adicional que se aplica somente quando a entidade a ser avaliada tratar-se de um prestador de serviços.</p>
<p><b>8.2.6</b> Defina as senhas/frases-senha para o primeiro uso e ao reiniciar com um valor exclusivo para cada usuário; a alteração deve ser imediata, após a primeira utilização.</p>	<p><b>8.2.6</b> Analise os procedimentos de senha e observe a equipe de segurança para verificar se as senhas/frases-senha iniciais para novos usuários e as senhas/frases-senha de reinicialização para usuários existentes são definidas com valor exclusivo para cada usuário e alteradas após a primeira utilização.</p>	<p>Se a mesma senha for usada para cada novo usuário, um usuário interno, ex-funcionário ou indivíduo mal-intencionado poderá conhecer ou descobrir facilmente essa senha e usá-la para obter acesso às contas.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.3</b> Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE são protegidos por autenticação multifatorial.</p> <p><b>Observação:</b> A autenticação multifatorial exige que, no mínimo, dois dos três métodos de autenticação (consultar Requisito 8.2 para ver descrições dos métodos de autenticação) sejam usados para autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado como autenticação multifatorial.</p>		<p>A autenticação multifatorial requer que o indivíduo apresente, no mínimo, duas formas distintas de autenticação (conforme descritas no Requisito 8.2), antes que o acesso seja concedido.</p> <p>A autenticação multifatorial fornece garantia adicional de que o indivíduo que procura obter acesso é quem ele afirma ser. Com a autenticação multifatorial, um invasor precisaria aceitar, pelo menos, dois mecanismos de autenticação diferentes, aumentando a dificuldade de transigência e reduzindo assim o risco.</p> <p>A autenticação multifatorial não é necessária nos níveis do sistema e do aplicativo para um componente de sistema em particular. A autenticação multifatorial pode ser realizada ao autenticar o acesso à rede em particular ou a um componente do sistema.</p> <p>Exemplos de tecnologias multifatoriais incluem, entre outros, autenticação remota e serviço dial-in (RADIUS) com token; sistema de controle de acesso ao controlador de acesso terminal (TACACS) com token; outras tecnologias que facilitam a autenticação multifatorial.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.3.1</b> Incorporar a autenticação multifatorial em todos os acessos que não utilizam console no CDE para funcionários com acesso administrativo.</p> <p><i>Observação: Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i></p>	<p><b>8.3.1.a</b> Analise as configurações de rede e/ou sistema, conforme o caso, para verificar se a autenticação multifatorial é necessária para todo o acesso administrativo ao CDE sem o uso de console.</p> <p><b>8.3.1.b</b> Observe um exemplo de login no CDE pela equipe do administrador e verifique se, pelo menos, dois dos três métodos de autenticação são usados.</p>	<p>Este requisito deve ser aplicado para toda a equipe com acesso administrativo ao CDE. Este requisito aplica-se somente ao pessoal com acesso administrativo e apenas para acesso ao CDE sem o uso de console; não se aplica às contas do sistema ou aplicativo que executam funções automatizadas.</p> <p>Se a entidade não usar segmentação para separar o CDE do restante da rede, o administrador poderá usar a autenticação multifatorial ao acessar o sistema ou a rede do CDE.</p> <p>Se não houver segmentação do CDE em relação ao restante da rede corporativa, o administrador precisará usar a autenticação multifatorial para conectar-se ao sistema do CDE a partir de uma rede não-CDE. A autenticação multifatorial pode ser implementada no nível da rede ou do sistema/aplicativo; não precisa ser em ambos. Se usar a autenticação multifatorial (Multi-Factor Authentication, MFA) ao fazer login na rede do CDE, o administrador não precisará usar MFA para acessar um determinado sistema ou aplicativo dentro do CDE.</p>
<p><b>8.3.2</b> Incorpore a autenticação multifatorial para todos os acessos remotos à rede (usuário e administrador, incluindo o acesso de terceiros para suporte ou manutenção) provenientes de fora da rede da entidade.</p>	<p><b>8.3.2.a</b> Analise as configurações do sistema para sistemas e servidores de acesso remoto e verifique se a autenticação de multifatorial é exigida para:</p> <ul style="list-style-type: none"> <li>• Todo acesso remoto pela equipe, tanto do usuário como do administrador, e</li> <li>• Todos os acessos remotos de fornecedores/terceiros (incluindo acesso aos componentes do sistema e aplicativos para suporte ou manutenção).</li> </ul> <p><b>8.3.2.b</b> Observe um exemplo de conexão remota à rede pela equipe (por exemplo, usuários e administradores) e verifique se, pelo menos, dois dos três métodos de autenticação são usados.</p>	<p>Esse requisito aplica-se a toda a equipe, inclusive usuários, administradores e fornecedores em geral (para suporte ou manutenção), com acesso remoto à rede, quando o acesso remoto possa levar ao acesso do CDE. Se o acesso remoto direcionar à rede de uma entidade que possui segmentação adequada, de forma tal que ao usuário remoto não seja possível acessar ou impactar o ambiente de dados do titular do cartão, a autenticação multifatorial para acesso remoto à rede não será exigida. No entanto, a autenticação multifatorial será exigida para qualquer acesso remoto a redes com acesso ao ambiente de dados do titular do cartão, a qual é recomendável para todo acesso remoto às redes da entidade.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.4</b> Registre e comunique os procedimentos e políticas de autenticação para todos os usuários, inclusive:</p> <ul style="list-style-type: none"> <li>• Orientação sobre selecionar credenciais fortes de autenticação</li> <li>• Orientação sobre como os usuários devem proteger suas credenciais de autenticação</li> <li>• Instruções para não reutilizar senhas anteriormente usadas</li> <li>• Instruções para alterar a senha se houver suspeita de que ela possa estar comprometida.</li> </ul>	<p><b>8.4.a</b> Analise os procedimentos e converse com os funcionários para verificar se os procedimentos e políticas de autenticação são distribuídos para todos os usuários.</p> <p><b>8.4.b</b> Analise as políticas e procedimentos de autenticação que são distribuídos aos usuários e verifique se eles incluem:</p> <ul style="list-style-type: none"> <li>• Orientação sobre selecionar credenciais fortes de autenticação</li> <li>• Orientação sobre como os usuários devem proteger suas credenciais de autenticação.</li> <li>• Instruções para os usuários não reutilizarem senhas anteriormente usadas</li> <li>• Instruções para alterar a senha se houver suspeita de que ela possa estar comprometida.</li> </ul> <p><b>8.4.c</b> Converse com alguns usuários para verificar se estão familiarizados com os procedimentos e políticas de autenticação.</p>	<p>Comunicar os procedimentos e políticas de autenticação/senha a todos os usuários contribui para que compreendam e cumpram as políticas.</p> <p>Por exemplo, a orientação sobre selecionar senhas fortes pode incluir sugestões para ajudar a equipe a selecionar senhas difíceis de adivinhar que não contenham palavras do dicionário e informações sobre o usuário (como ID do usuário, nomes de familiares, data de aniversário, etc.). A orientação para proteger as credenciais de autenticação pode incluir não anotar senhas ou salvá-las em arquivos não seguros e estar alerta a indivíduos mal-intencionados que possam tentar explorar suas senhas (por exemplo, ligando para um funcionário e perguntando sua senha para que ele possa “resolver um problema”).</p> <p>Instruir os usuários a alterar suas senhas se houver a possibilidade de ela não ser mais segura pode evitar que usuários mal-intencionados usem uma senha legítima para obter acesso não autorizado.</p>
<p><b>8.5</b> Não use IDs de grupos, compartilhados ou genéricos, senhas ou outros métodos de autenticação conforme segue:</p> <ul style="list-style-type: none"> <li>• IDs genéricos de usuários são desativados ou removidos.</li> <li>• IDs de usuários compartilhados não existem para a administração do sistema e outras funções críticas.</li> <li>• IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema.</li> </ul>	<p><b>8.5.a</b> Para obter uma amostra dos componentes do sistema, analise as listas de ID do usuário para verificar o seguinte:</p> <ul style="list-style-type: none"> <li>• IDs genéricos de usuários são desativados ou removidos.</li> <li>• IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas não existem.</li> <li>• IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema.</li> </ul> <p><b>8.5.b</b> Analise as políticas e procedimentos de autenticação para verificar se o uso de senhas e/ou IDs compartilhadas e de grupo ou outros métodos de autenticação são explicitamente proibidos.</p> <p><b>8.5.c</b> Converse com os administradores do sistema para verificar se as senhas e/ou IDs de grupo ou compartilhados ou outros métodos de autenticação não são distribuídos, mesmo se forem solicitados.</p>	<p>Se vários usuários compartilharem as mesmas credenciais de autenticação (conta e senha, por exemplo), torna-se impossível controlar o acesso ao sistema e atividades de um indivíduo. Isso evita que uma entidade assuma a responsabilidade de, ou faça um registro eficaz das ações de um indivíduo, pois uma determinada ação pode ter sido executada por qualquer pessoa no grupo que saiba as credenciais de autenticação.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>8.5.1 Requisito adicional, somente para prestadores de serviços:</b> Os prestadores de serviço com acesso remoto ao local do cliente (por exemplo, para suporte de servidores ou sistemas POS) devem usar uma credencial de autenticação exclusiva (como uma senha/frase) para cada cliente.</p> <p><b>Observação:</b> Este requisito não tem o objetivo de se aplicar a provedores de hospedagem compartilhada que acessam seu próprio ambiente de hospedagem, onde vários ambientes do cliente são hospedados.</p>	<p><b>8.5.1. Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Analise as políticas e procedimentos de autenticação e converse com os funcionários para verificar se são usadas credenciais de autenticação diferentes para acesso a cada cliente.</p>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>Para prevenir o comprometimento de vários clientes devido ao uso de um conjunto único de credenciais, os fornecedores com contas de acesso remoto aos ambientes do cliente devem usar uma credencial de autenticação diferente para cada cliente.</p> <p>Tecnologias, como mecanismos multifatoriais, que oferecem uma credencial única para cada conexão (por exemplo, por meio de uma senha de uso comum) também podem atender ao objetivo deste requisito.</p>
<p><b>8.6</b> Onde forem usados outros mecanismos de autenticação (por exemplo, tokens de segurança físicos ou virtuais, smart cards, certificados, etc.), o uso destes mecanismos deve ser atribuído conforme segue:</p> <ul style="list-style-type: none"> <li>Os mecanismos de autenticação devem ser atribuídos a uma conta individual e não compartilhados entre várias contas.</li> <li>Controles físicos e/ou virtuais devem ser implementados para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso.</li> </ul>	<p><b>8.6.a</b> Analise as políticas e procedimentos de autenticação para verificar se os procedimentos para usar os mecanismos de autenticação, como tokens de segurança físicos, smart cards e certificados estão definidos e incluem:</p> <ul style="list-style-type: none"> <li>Os mecanismos de autenticação são atribuídos a uma conta individual e não compartilhados entre várias contas.</li> <li>Controles físicos e/ou virtuais estão definidos para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso.</li> </ul>	<p>Se os mecanismos de autenticação do usuário, como tokens, smart cards e certificados puderem ser usados por várias contas, pode ser impossível identificar o indivíduo que utiliza o mecanismo de autenticação. Ter controles físicos e/ou virtuais (por exemplo, um PIN, dados biométricos ou uma senha) para identificar exclusivamente o usuário da conta evitará que usuários não autorizados obtenham acesso através do uso de um mecanismo de autenticação compartilhado.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>8.6.b</b> Converse com a equipe de segurança para verificar se os mecanismos de autenticação são atribuídos a uma conta e não compartilhados entre várias contas.</p> <p><b>8.6.c</b> Analise os ajustes da configuração do sistema e/ou os controles físicos, conforme aplicável, para verificar se os controles estão implementados para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso.</p>	
<p><b>8.7</b> Todos os acessos a qualquer banco de dados que contenha dados do titular do cartão (inclusive acesso por meio de aplicativos, por administradores e demais usuários) são restritos, conforme segue:</p> <ul style="list-style-type: none"> <li>• Todos os acessos, consultas e ações do usuário no banco de dados ocorrem através de métodos programáticos.</li> <li>• Apenas os administradores do banco de dados podem acessar diretamente ou consultar o banco de dados.</li> <li>• Os IDs dos aplicativos para os aplicativos do banco de dados só podem ser usados pelos aplicativos (e não por usuários individuais ou outros processos sem aplicativo).</li> </ul>	<p><b>8.7.a</b> Analise as definições de configuração do aplicativo e do banco de dados para verificar se todos os usuários são autenticados antes do acesso.</p> <p><b>8.7.b</b> Analise as definições de configuração do aplicativo e do banco de dados para verificar se todos os acessos, consultas e ações dos usuários (por exemplo, mover, copiar, excluir) nos bancos de dados são por meio apenas de métodos programáticos (por exemplo, através dos procedimentos armazenados).</p> <p><b>8.7.c</b> Analise as configurações do controle de acesso do banco de dados e as definições de configuração do aplicativo e do banco de dados para verificar se o acesso direto ou consultas ao banco de dados são restritos aos administradores.</p> <p><b>8.7.d</b> Analise as configurações do controle de acesso do banco de dados, as definições de configuração do aplicativo do banco de dados e os IDs dos aplicativos relacionados para verificar se os IDs dos aplicativos podem ser usados somente pelos aplicativos (e não apenas por usuários individuais ou outros processos).</p>	<p>Sem autenticação do usuário para acesso a bancos de dados e aplicativos, o potencial para acesso não autorizado ou mal-intencionado aumenta e esse acesso não pode ser registrado, pois o usuário não foi autenticado e, assim, não é conhecido pelo sistema. Além disso, o acesso ao banco de dados só deve ser concedido por meio de métodos programáticos (por exemplo, por meio de procedimentos armazenados) e não por acesso direto ao banco de dados por usuários finais (exceto para DBAs, que podem precisar de acesso direto ao banco de dados para as tarefas administrativas).</p>
<p><b>8.8</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para identificação e autenticação estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>8.8</b> Analise a documentação e converse com os funcionários para verificar se as políticas de segurança e procedimentos operacionais para identificação e autenticação estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para controlar continuamente as identificações e autorizações.</p>

## Requisito 9: Restringir o acesso físico aos dados do titular do cartão

Qualquer acesso físico aos dados ou sistemas que armazenam dados do titular do cartão conferem a oportunidade para que pessoas acessem dispositivos ou dados e removam sistemas ou cópias impressas, e deve ser restrito de forma adequada. Para as finalidades do Requisito 9, "funcionário" refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias e prestadores de serviços e consultores que atuam com presença física no endereço da entidade. Um "visitante" refere-se a um fornecedor, convidado de um funcionário, equipes de serviço ou qualquer pessoa que precise adentrar as dependências por um breve período, normalmente um dia, no máximo. "Mídia" refere-se a todas as mídias impressas ou eletrônicas que contenham dados do titular do cartão.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.1</b> Use controles de entrada facilitados e adequados para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do titular do cartão.</p>	<p><b>9.1</b> Verifique a existência dos controles de segurança física em cada ambiente com computador, central de dados e outras áreas físicas com sistemas no ambiente de dados do titular do cartão.</p> <ul style="list-style-type: none"> <li>• Verifique se o acesso é controlado com leitores de credenciais ou outros dispositivos, incluindo credenciais autorizadas e bloqueio e chave.</li> <li>• Observe a tentativa de login do administrador do sistema em consoles visando aos sistemas selecionados aleatoriamente no ambiente de dados do titular do cartão e verifique se eles estão "bloqueados" para impedir o uso não autorizado.</li> </ul>	<p>Sem controles físicos de acesso, como sistemas de crachás e controles de porta, usuários não autorizados podem facilmente obter acesso às instalações para roubar, desativar, interromper ou destruir sistemas críticos e dados do titular do cartão.</p> <p>Bloquear telas de logon em consoles evita que pessoas não autorizadas obtenham acesso a informações confidenciais, alterando as configurações do sistema, introduzindo vulnerabilidades na rede ou destruindo registros.</p>
<p><b>9.1.1</b> Use câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis. Analise os dados coletados e relacione com outras entradas. Armazene, por pelo menos três meses, a menos que seja restringido de outra forma pela lei.</p> <p><b>Observação:</b> "Áreas confidenciais" referem-se a qualquer central de dados, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam dados do titular do cartão. Isso exclui áreas voltadas ao público nas quais há somente terminais do ponto de venda presentes, como as áreas dos caixas em uma loja de varejo.</p>	<p><b>9.1.1.a</b> Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) foram implantados para monitorar os pontos de entrada/saída das áreas sensíveis.</p> <p><b>9.1.1.b</b> Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) estão protegidos contra adulteração ou desativação.</p>	<p>Ao investigar violações físicas, esses controles podem ajudar a identificar indivíduos que acessaram fisicamente as áreas confidenciais, bem como quando eles entraram e saíram.</p> <p>Criminosos que tentam obter acesso físico às áreas confidenciais muitas vezes tentarão desativar ou desviar os controles de monitoramento. Para proteger estes controles contra adulterações, câmeras de vídeo podem ser posicionadas de forma que fiquem fora de alcance e/ou sejam monitoradas para detectar falsificações. Da mesma forma, os mecanismos de controle de acesso podem ser monitorados ou ter proteções físicas instaladas para evitar que sejam danificados ou desativados por indivíduos mal-intencionados.</p> <p style="text-align: right;"><i>(Continua na próxima página)</i></p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>9.1.1.c</b> Verifique se câmeras de vídeo e/ou outros mecanismos de controle de acesso são monitorados, e se os dados são armazenados por, pelo menos, três meses.</p>	<p>Exemplos de áreas confidenciais incluem salas do servidor do banco de dados corporativo, salas do setor administrativo em local de revenda que armazene dados do titular do cartão e áreas de armazenamento de grandes quantidades de dados do titular do cartão. As áreas confidenciais devem ser identificadas por cada organização para garantir que os controles de monitoramento físicos adequados sejam implementados.</p>
<p><b>9.1.2</b> Implemente controles físicos e/ou virtuais para restringir o acesso a pontos de rede acessíveis publicamente.</p> <p><i>Por exemplo, pontos de rede localizados em áreas públicas e áreas acessíveis a visitantes podem ser desativados e somente ativados quando o acesso à rede é explicitamente autorizado. Alternativamente, processos podem ser implementados para garantir que os visitantes sempre sejam acompanhados nas áreas com pontos de rede ativos.</i></p>	<p><b>9.1.2</b> Converse com os funcionários responsáveis e observe os locais de pontos de rede publicamente acessíveis para verificar se controles físicos e/ou virtuais estão implementados para restringir o acesso a estes pontos de rede.</p>	<p>Restringir o acesso aos pontos de rede (ou portas de rede) evita que indivíduos mal-intencionados se conectem em pontos de rede prontamente disponíveis e obtenham acesso aos recursos de rede internos.</p> <p>Se forem usados controles físicos ou virtuais, ou os dois, eles devem ser suficientes para evitar que um indivíduo ou dispositivo não autorizado consiga se conectar à rede.</p>
<p><b>9.1.3</b> Restrinja o acesso físico a pontos sem fio de acesso, gateways, dispositivos portáteis, hardwares de comunicação/rede e linhas de telecomunicação.</p>	<p><b>9.1.3</b> Verifique se o acesso físico a pontos sem fio de acesso, gateways, dispositivos portáteis, hardwares de comunicação/rede e linhas de telecomunicação é restrito adequadamente.</p>	<p>Sem segurança no acesso a componentes e dispositivos sem fio, indivíduos mal-intencionados podem usar os dispositivos sem fio da sua empresa que não estejam sendo utilizados para acessar os recursos de rede ou até para conectar seus próprios dispositivos à rede sem fio para obter acesso não autorizado. Além disso, fazer a segurança dos materiais de comunicação e rede evita que usuários mal-intencionados interceptem o tráfego da rede ou conectem fisicamente seus próprios dispositivos aos recursos de rede com fio.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.2</b> Desenvolva procedimentos para diferenciar facilmente a equipe interna dos visitantes e inclua:</p> <ul style="list-style-type: none"> <li>• Identificação de funcionários e visitantes no local (por exemplo, crachás de identificação)</li> <li>• Modificações nos requisitos de acesso</li> <li>• Anular ou excluir identificações de funcionários que se desligaram da empresa e de visitantes que encerraram sua atividade (como crachás de identificação).</li> </ul>	<p><b>9.2</b> Analise os processos documentados para verificar se estão definidos procedimentos para identificar e diferenciar os funcionários dos visitantes.</p> <ul style="list-style-type: none"> <li>• Verifique se os processos incluem o seguinte:</li> <li>• Identificação de funcionários e de visitantes no local (por exemplo, crachás de identificação),</li> <li>• Modificar os requisitos de acesso e</li> <li>• Anular identificações de funcionários que se desligaram da empresa e de visitantes que encerraram sua atividade (como crachás de identificação)</li> </ul> <p><b>9.2.b</b> Analise os métodos de identificação (como crachás de identificação) e observe os processos para identificar e diferenciar os funcionários dos visitantes, para verificar se:</p> <ul style="list-style-type: none"> <li>• Os visitantes são claramente identificados, e</li> <li>• É fácil diferenciar os visitantes dos membros da equipe interna.</li> </ul> <p><b>9.2.c</b> Verifique se o acesso ao processo de identificação (como um sistema de crachás) é limitado a funcionários autorizados.</p>	<p>Identificar visitantes autorizados para que sejam facilmente distinguidos dos funcionários do local evita que visitantes não autorizados acessem áreas que contenham dados do titular do cartão.</p>
<p><b>9.3</b> Controle o acesso físico dos funcionários às áreas sensíveis, conforme segue:</p> <ul style="list-style-type: none"> <li>• O acesso deve ser autorizado e com base na função do indivíduo.</li> <li>• O acesso é anulado imediatamente ao término da atividade e todos os mecanismos de acesso físico, como chaves, cartões de acesso, etc., são devolvidos e desativados.</li> </ul>	<p><b>9.3.a</b> Para obter uma amostra de funcionários com acesso físico às áreas sensíveis, converse com o funcionário responsável e observe as listas de controle de acesso para verificar se:</p> <ul style="list-style-type: none"> <li>• O acesso à área sensível é autorizado.</li> <li>• O acesso é necessário para a função da pessoa.</li> </ul> <p><b>9.3.b</b> Observe o acesso dos funcionários às áreas sensíveis para verificar se todos são autorizados antes de receberem acesso.</p> <p><b>9.3.c</b> Selecione exemplos de funcionários recentemente desligados e revise as listas de controle de acesso para verificar se os mesmos não têm acesso físico às áreas sensíveis.</p>	<p>Controlar o acesso físico às áreas sensíveis contribui para garantir que o acesso será concedido somente aos funcionários autorizados com necessidade comercial legítima.</p> <p>Quando um funcionário deixa a empresa, todos os mecanismos de acesso físico devem ser devolvidos e desativados imediatamente (assim que possível) após a saída, para garantir que ele não tenha acesso físico às áreas sensíveis quando não for mais funcionário da empresa.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.4</b> Implemente procedimentos para identificar e autorizar visitantes.</p> <p>Os procedimentos devem incluir o seguinte:</p>	<p><b>9.4</b> Verifique se os controles de acesso e autorização dos visitantes estão implementados da seguinte forma:</p>	<p>O controle de visitantes é importante para reduzir a possibilidade de pessoas não autorizadas e mal-intencionadas obterem acesso às instalações (e possivelmente aos dados do titular do cartão).</p>
<p><b>9.4.1</b> Os visitantes devem obter autorização antes de entrar e serem sempre acompanhados em áreas nas quais os dados do titular do cartão são processados ou mantidos.</p>	<p><b>9.4.1.a</b> Observe os procedimentos e questione os funcionários para verificar se os visitantes devem obter autorização antes de entrar e serem sempre acompanhados em áreas nas quais os dados do titular do cartão são processados ou mantidos.</p> <p><b>9.4.1.b</b> Observe o uso dos crachás de visitante ou outra identificação para verificar se um crachá de token físico não permite acesso desacompanhado a áreas físicas onde os dados do titular do cartão são processados ou mantidos.</p>	<p>Os controles de visitantes garantem que eles sejam identificados como visitantes, de forma que os funcionários possam monitorar suas atividades e que o acesso esteja restrito somente à duração de sua visita.</p> <p>Garantir que os crachás de visitantes sejam devolvidos ao final de sua visita evita que pessoas mal-intencionadas utilizem uma passagem anteriormente autorizada para obter acesso físico ao prédio após o término de sua visita.</p>
<p><b>9.4.2</b> Os visitantes são identificados e recebem um crachá ou outra identificação que expira e que distingue visivelmente os visitantes dos funcionários internos.</p>	<p><b>9.4.2.a</b> Observe as pessoas na instalação para verificar o uso dos crachás de visitante ou outra identificação e se é fácil distinguir os visitantes dos funcionários.</p> <p><b>9.4.2.b</b> Verifique se os crachás de visitante ou outra identificação têm validade.</p>	<p>Um log de visitantes documentando as informações mínimas sobre eles é de manutenção fácil e barata e ajuda a identificar o acesso físico a um edifício ou a uma sala e um possível acesso aos dados do titular do cartão.</p>
<p><b>9.4.3</b> É solicitado que os visitantes apresentem o crachá ou identificação antes de sair das dependências ou na data do vencimento.</p>	<p><b>9.4.3</b> Observe os visitantes que saem das dependências para verificar se é solicitado que eles apresentem seu crachá ou outra identificação na saída ou ao vencimento.</p>	
<p><b>9.4.4</b> Um registro de visitantes é usado para manter uma trilha de auditoria da atividade do visitante nas dependências, assim como aos ambientes com computador e centrais de dados onde os dados do titular do cartão são armazenados ou transmitidos.</p> <p>Documente no registro o nome do</p>	<p><b>9.4.4.a</b> Verifique se um registro de visitantes está sendo usado para registrar o acesso físico às dependências, assim como aos ambientes com computador e centrais de dados onde os dados do titular do cartão são armazenados ou transmitidos.</p> <p><b>9.4.4.b</b> Verifique se o registro contém:</p> <ul style="list-style-type: none"> <li>• O nome do visitante,</li> <li>• A empresa representada, e</li> <li>• O funcionário que autoriza o acesso físico.</li> </ul>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>visitante, a empresa representada e o funcionário que autoriza o acesso físico.</p> <p>Armazene esse registro por pelo menos três meses, a menos que seja restringido de outra forma pela lei.</p>	<p><b>9.4.4.c</b> Verifique se o registro é mantido por pelo menos três meses.</p>	
<p><b>9.5</b> Proteja toda a mídia fisicamente.</p>	<p><b>9.5</b> Verifique se os procedimentos para proteger os dados do titular do cartão incluem controles para proteger fisicamente todas as mídias (incluindo, entre outros, a computadores, mídias eletrônicas removíveis, recebimentos de documentos impressos, relatórios impressos e faxes).</p>	<p>Os controles para proteger fisicamente as mídias têm o objetivo de evitar que pessoas não autorizadas obtenham acesso aos dados do titular do cartão em qualquer tipo de mídia. Os dados do titular do cartão estarão suscetíveis a visualização, cópia ou digitalização não autorizada caso estejam desprotegidos enquanto estiverem em mídia portátil, forem impressos ou deixados na mesa de alguém.</p>
<p><b>9.5.1</b> Armazene backups de mídia em um local seguro, preferencialmente em outras instalações, como um lugar alternativo de backup ou uma instalação comercial de armazenamento. Analise a segurança do local pelo menos uma vez por ano.</p>	<p><b>9.5.1</b> Verifique se o local de armazenamento é analisado, pelo menos, uma vez por ano para confirmar se o armazenamento das mídias de backup está protegido.</p>	<p>Se armazenados em um local não protegido, os backups que contêm dados do titular do cartão podem ser facilmente perdidos, roubados ou copiados com más intenções.</p> <p>Revisar periodicamente o local de armazenamento permite que a organização resolva problemas de segurança em tempo hábil, minimizando o potencial de risco.</p>
<p><b>9.6</b> Mantenha controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia, incluindo o seguinte:</p>	<p><b>9.6</b> Verifique se há uma política para controlar a distribuição de mídias que contêm dados do titular do cartão e se a política abrange todas as mídias distribuídas, incluindo as distribuídas às pessoas.</p>	<p>Procedimentos e processos ajudam a proteger os dados do titular do cartão em mídias distribuídas a usuários internos e/ou externos. Sem tais procedimentos, os dados poderão ser perdidos ou roubados e usados para fins fraudulentos.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.6.1</b> Classifique a mídia para que a confidencialidade dos dados possa ser determinada.</p>	<p><b>9.6.1</b> Verifique se toda a mídia foi classificada para que a confidencialidade dos dados possa ser determinada.</p>	<p>É importante que a mídia seja identificada para que seu status de classificação possa ser facilmente discernível. A mídia não identificada como confidencial pode não ser protegida adequadamente ou ser roubada.</p> <p><b>Observação:</b> Isto não significa que as mídias precisam ter anexado um rótulo “Confidencial”; o objetivo é que a organização tenha identificado a mídia que contém dados confidenciais para que possa protegê-los.</p>
<p><b>9.6.2</b> Envie a mídia via mensageiro seguro ou outro método de entrega que possa ser monitorado com precisão.</p>	<p><b>9.6.2.a</b> Converse com os funcionários e analise os registros para verificar se toda a mídia enviada para fora das dependências é registrada e encaminhada via mensageiro seguro ou outro método de entrega que possa ser monitorado.</p> <p><b>9.6.2.b</b> Selecione um exemplo recente de vários dias de registros de monitoramento externo para todas as mídias e verifique se os detalhes de rastreamento estão documentados.</p>	<p>A mídia pode ser perdida ou roubada se for enviada por um método não rastreável, como remessa postal. O uso de mensageiros seguros para entregar mídias que contenham dados do titular do cartão permite que as organizações usem seus sistemas de rastreamento para manter inventário e localização dos envios.</p>
<p><b>9.6.3</b> Certifique-se de que o gerenciamento aprova quaisquer e todas as mídias que são movidas de uma área segura (incluindo quando as mídias forem distribuídas às pessoas).</p>	<p><b>9.6.3</b> Selecione um exemplo recente de vários dias de logs de monitoramento externo para todas as mídias. A partir da análise dos registros e questionamentos com os funcionários responsáveis, verifique se é obtida a autorização adequada do gerenciamento sempre que as mídias forem movidas de uma área segura (incluindo quando as mídias forem distribuídas às pessoas).</p>	<p>Sem um processo rigoroso para garantir que todos os movimentos de mídia sejam aprovados antes que ela seja removida das áreas seguras, a mídia não seria rastreada ou adequadamente protegida e sua localização seria desconhecida, levando a mídias perdidas ou roubadas.</p>
<p><b>9.7</b> Mantenha um controle rigoroso sobre o armazenamento e a acessibilidade das mídias.</p>	<p><b>9.7</b> Obtenha e analise a política para controlar o armazenamento e a manutenção dos documentos impressos e mídias eletrônicas e verifique se a política requer inventários de mídia periódicos.</p>	<p>Sem métodos cuidadosos de inventário e controles de armazenamento, mídias roubadas ou ausentes podem passar despercebidas por tempo indefinido.</p>
<p><b>9.7.1</b> Mantenha adequadamente os registros do inventário de todas as mídias e realize inventários das mídias pelo menos uma vez por ano.</p>	<p><b>9.7.1</b> Revise o registro do inventário das mídias para verificar se os registros são mantidos e se os inventários de mídia são realizados pelo menos uma vez por ano.</p>	<p>Se a mídia não passar por inventário, mídias roubadas ou perdidas podem passar despercebidas por bastante tempo.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.8</b> Destrua as mídias quando não forem mais necessárias por motivos legais ou de negócios, conforme segue:</p>	<p><b>9.8</b> Analise a política de destruição periódica das mídias e verifique se ela abrange todas as mídias e se define requisitos para o seguinte:</p> <ul style="list-style-type: none"> <li>• Materiais impressos devem ser triturados, incinerados ou amassados de forma que haja uma garantia razoável de que esses materiais não possam ser recuperados.</li> <li>• Os contêineres de armazenamento usados para os materiais a serem destruídos devem estar seguros.</li> <li>• Os dados dos titulares de cartão na mídia eletrônica devem ser processados de modo irrecuperável (por exemplo, através de um programa de limpeza segura em conformidade com os padrões aceitos de indústria para exclusão segura, ou destruindo fisicamente a mídia).</li> </ul>	<p>Se as etapas não forem seguidas para destruir as informações contidas em discos rígidos, drives portáteis, CD/DVDs ou papéis antes do descarte, indivíduos mal-intencionados podem estar aptos a recuperar as informações da mídia descartada, levando ao comprometimento dos dados. Por exemplo, indivíduos mal-intencionados podem usar uma técnica conhecida como “dumpster diving”, na qual eles pesquisam em lixeiras e usam as informações encontradas para iniciar um invasão.</p> <p>Proteger os contêineres de armazenamento usados para os materiais que serão destruídos evita que informações confidenciais sejam capturadas enquanto os materiais estão sendo coletados. Por exemplo, contêineres “a serem triturados” podem ter um bloqueio que evita o acesso a seu conteúdo ou que previna fisicamente o acesso para dentro do contêiner.</p> <p>Exemplos de métodos para destruir mídias eletrônicas incluem limpeza segura, desmagnetização ou destruição física (como esmagar ou triturar os discos rígidos).</p>
<p><b>9.8.1</b> Triture, incinere ou amasse materiais impressos para que os dados do titular do cartão não possam ser recuperados. Contêineres de armazenamento usados para os materiais a serem destruídos.</p>	<p><b>9.8.1.a</b> Converse com os funcionários e analise os procedimentos para verificar se os materiais impressos são picotados, triturados, incinerados ou amassados para que haja garantia razoável de que não possam ser reconstituídos.</p> <p><b>9.8.1.b</b> Analise os contêineres de armazenamento usados para os materiais que contêm informações a serem destruídas para verificar se são seguros.</p>	<p>Exemplos de métodos para destruir mídias eletrônicas incluem limpeza segura, desmagnetização ou destruição física (como esmagar ou triturar os discos rígidos).</p>
<p><b>9.8.2</b> Torne os dados do titular do cartão nas mídias eletrônicas irrecuperáveis para que esses dados não possam ser reconstituídos.</p>	<p><b>9.8.2</b> Verifique se os dados do titular do cartão nas mídias eletrônicas apresentam-se irrecuperáveis (p. ex., via programa de limpeza segura, de acordo com os padrões aceitos pelo setor quanto à exclusão segura ou, de outra forma, pela destruição física das mídias).</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.9</b> Proteja contra falsificação e substituição os dispositivos que capturam os dados do cartão de pagamento por meio de interação física direta com o cartão.</p> <p><b>Observação:</b> Estes requisitos se aplicam aos dispositivos de leitura do cartão usados em transações com a presença do cartão (ou seja, de passar ou inserir) no ponto de venda. Este requisito não tem o objetivo de se aplicar aos componentes de entrada de chave manual, como teclados de computador e teclados POS.</p>	<p><b>9.9</b> Analise as políticas e procedimentos para verificar se eles incluem:</p> <ul style="list-style-type: none"> <li>• Manter uma lista de dispositivos</li> <li>• Inspeccionar periodicamente os dispositivos para identificar falsificações ou substituições</li> <li>• Treinar os funcionários para que reconheçam comportamentos suspeitos e para reportar a falsificação ou substituição de dispositivos.</li> </ul>	<p>Criminosos tentam roubar os dados do titular do cartão roubando e/ou manipulando os terminais e dispositivos de leitura do cartão. Por exemplo, eles tentarão roubar os dispositivos para que eles possam saber como arrombá-los e eles geralmente tentam validar os dispositivos com dispositivos fraudulentos que enviam a eles as informações do cartão de pagamento sempre que o cartão é inserido. Os criminosos também tentarão adicionar componentes de "espionagem" na parte externa dos dispositivos, que são designados para capturar os detalhes do cartão antes mesmo de ser inserido, por exemplo, anexando um leitor de cartão adicional em cima do leitor do cartão original para que os detalhes do cartão sejam capturados duas vezes: uma vez pelo componente do criminoso e depois pelo componente legítimo do dispositivo. Dessa forma, as transações ainda podem ser concluídas sem interrupção enquanto o criminoso está "espiando" as informações do cartão durante o processo.</p> <p>Este requisito é recomendado, mas não exigido, para componentes de entrada de chave manual, como teclados de computador e teclados POS.</p> <p>Melhores práticas adicionais sobre a prevenção de espionagem estão disponíveis no site do PCI SSC.</p>
<p><b>9.9.1</b> Mantenha uma lista atualizada de dispositivos. A lista deve incluir o seguinte:</p> <ul style="list-style-type: none"> <li>• Marca, modelo do dispositivo</li> <li>• Localização do dispositivo (por exemplo, o endereço do local ou instalação onde o dispositivo está localizado)</li> <li>• Número de série do dispositivo ou</li> </ul>	<p><b>9.9.1.a</b> Analise a lista de dispositivos para verificar se ela inclui:</p> <ul style="list-style-type: none"> <li>• Marca, modelo do dispositivo</li> <li>• Localização do dispositivo (por exemplo, o endereço do local ou instalação onde o dispositivo está localizado)</li> <li>• Número de série do dispositivo ou outro método de identificação exclusivo.</li> </ul> <p><b>9.9.1.b</b> Selecione uma amostra de dispositivos a partir da lista e observe os dispositivos e locais de dispositivos para verificar se a lista está correta e atualizada.</p>	<p>Manter uma lista atualizada de dispositivos ajuda uma organização a controlar onde os dispositivos devem estar e rapidamente identificar se um deles está faltando ou perdido.</p> <p>O método para manter uma lista de dispositivos pode ser automatizado (por exemplo, um sistema de gerenciamento de dispositivos) ou manual (por exemplo, documentado em registros de papel ou eletrônicos). Para os dispositivos em trânsito, a localização pode incluir o nome do funcionário</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>outro método de identificação exclusivo.</p>	<p><b>9.9.1.c</b> Converse com os funcionários para verificar se a lista de dispositivos é atualizada quando dispositivos são adicionados, realocados, retirados, etc.</p>	<p>para quem o dispositivo é concedido.</p>
<p><b>9.9.2</b> Inspeccione periodicamente as superfícies dos dispositivos para detectar adulteração (por exemplo, adição de espões aos dispositivos), ou substituição (por exemplo, verificando o número de série ou outras características do dispositivo para verificar se ele não foi trocado por um dispositivo fraudulento).</p> <p><b>Observação:</b> <i>exemplos de sinais de que um dispositivo possa ter sido adulterado ou substituído incluem apêndices inesperados ou cabos conectados ao dispositivo, rótulos de segurança alterados ou ausentes, revestimento quebrado ou de cor diferente, ou alterações no número de série ou outras marcas externas.</i></p>	<p><b>9.9.2.a</b> Analise os procedimentos documentados para verificar se os processos estão definidos para incluir o que segue:</p> <ul style="list-style-type: none"> <li>• Procedimentos para inspecionar os dispositivos</li> <li>• Frequência de inspeções.</li> </ul> <p><b>9.9.2.b</b> Converse com os funcionários responsáveis e observe os processos de inspeção para verificar se:</p> <ul style="list-style-type: none"> <li>• Os funcionários conhecem os procedimentos de inspeção dos dispositivos.</li> <li>• Todos os dispositivos são inspecionados periodicamente para evidência de adulteração e substituição.</li> </ul>	<p>As inspeções regulares dos dispositivos ajudarão as organizações a detectar mais rapidamente adulterações ou substituições de um dispositivo e, então, minimizar o possível impacto de usar dispositivos fraudulentos.</p> <p>O tipo de inspeção dependerá do dispositivo, por exemplo, fotografias de dispositivos que são conhecidos por serem seguros podem ser usadas para comparar a aparência atual de um dispositivo com sua aparência original para ver se ela mudou. Outra opção pode ser usar uma caneta marcadora segura, como um marcador de luz UV, para marcar as superfícies e aberturas do dispositivo para que qualquer adulteração ou substituição seja aparente. Os criminosos frequentemente substituirão a estrutura externa de um dispositivo para ocultar sua adulteração e estes métodos podem ajudar a detectar tais atividades. Os fornecedores dos dispositivos também podem fornecer orientações de segurança e guias “como fazer” para ajudar a determinar se o dispositivo foi adulterado.</p> <p>A frequência de inspeções dependerá de fatores como o local do dispositivo e se este é frequentado ou não. Por exemplo, dispositivos deixados em áreas públicas sem supervisão pelo funcionário pode ter inspeções mais frequentes do que dispositivos mantidos em áreas seguras ou que sejam supervisionados quando eles estão acessíveis ao público. O tipo e frequência de inspeções são determinados pelo comerciante, conforme definido pelo seu processo anual de avaliação de riscos.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>9.9.3</b> Treine os funcionários para que estejam cientes das tentativas de adulteração ou substituição de dispositivos. O treinamento deve incluir o seguinte:</p> <ul style="list-style-type: none"> <li>• Verifique a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos.</li> <li>• Não instale, substitua ou devolva dispositivos sem verificação.</li> <li>• Esteja atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas).</li> <li>• Reporte comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança).</li> </ul>	<p><b>9.9.3.a</b> Analise os materiais de treinamento para os funcionários dos locais de ponto de venda para verificar se eles incluem o treinamento do seguinte:</p> <ul style="list-style-type: none"> <li>• Verificar a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos</li> <li>• Não instalar, substituir ou devolver dispositivos sem verificação</li> <li>• Estar atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas)</li> <li>• Reportar comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança).</li> </ul> <p><b>9.9.3.b</b> Converse com alguns funcionários nos locais de ponto de venda para verificar se ele receberam treinamento e se estão cientes dos procedimentos para o seguinte:</p> <ul style="list-style-type: none"> <li>• Verificar a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos</li> <li>• Não instalar, substituir ou devolver dispositivos sem verificação</li> <li>• Estar atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas)</li> <li>• Reportar comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança).</li> </ul>	<p>Os criminosos frequentemente afirmam ser da equipe de manutenção autorizada para obter acesso aos dispositivos POS. Todos os terceiros que solicitarem acesso aos dispositivos devem ser sempre verificados antes de terem o acesso concedido, por exemplo, verificando com o gerenciamento ou telefonando para a empresa de manutenção do POS (como o fornecedor ou adquirente) para verificação. Muitos criminosos tentarão enganar os funcionários se vestindo para a função (por exemplo, carregando caixas de ferramentas e vestidos com uniformes de trabalho) e também podem saber sobre os locais dos dispositivos, por isso é importante que os funcionários sejam treinados para seguir sempre os procedimentos.</p> <p>Outro truque que os criminosos gostam de usar é enviar um “novo” sistema de POS com instruções para trocá-lo com o sistema legítimo e “devolver” o sistema legítimo para um endereço específico. Os criminosos podem ainda oferecer a postagem de retorno já que querem muito colocar suas mãos nestes dispositivos. Os funcionários sempre verificam com o gerente ou fornecedor se o dispositivo é legítimo e se veio de uma fonte confiável antes de instalá-lo ou usá-lo para negócios.</p>
<p><b>9.10</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para restringir o acesso físico aos dados do titular do cartão estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>9.10</b> Analise a documentação e questione os funcionários para verificar se as políticas de segurança e procedimentos operacionais para restringir o acesso físico aos dados do titular do cartão estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para restringir o acesso físico dos dados do titular do cartão e sistemas CDE continuamente.</p>

## Monitorar e testar as redes regularmente

### **Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão**

Mecanismos de registro e a capacidade de monitorar as atividades dos usuários são fundamentais na prevenção, detecção ou minimização do impacto do comprometimento dos dados. A presença de registros em todos os ambientes permite o monitoramento, o alerta e a análise completa quando algo dá errado. Determinar a causa de um comprometimento é muito difícil, se não impossível, sem registros das atividades do sistema.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<b>10.1</b> Implemente trilhas de auditoria para ligar todos os acessos aos componentes do sistema para cada usuário individual.	<b>10.1</b> Verifique, através da observação e questionando o administrador do sistema, se: <ul style="list-style-type: none"> <li>• Trilhas de auditoria estão habilitadas e ativas para os componentes do sistema.</li> <li>• O acesso aos componentes do sistema está ligado aos usuários individuais.</li> </ul>	É essencial ter um processo ou sistema que vincule o acesso do usuário aos componentes do sistema acessados. Esse sistema gera logs de auditoria e oferece a capacidade de rastrear as atividades suspeitas de um usuário específico.
<b>10.2</b> Implemente trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:	<b>10.2</b> Por meio de entrevistas do funcionário responsável, observação de registros de auditoria e análise de suas configurações, desempenhe o seguinte:	Gerar trilhas de auditoria de atividades suspeitas alerta o administrador do sistema, envia dados a outros mecanismos de monitoramento (como sistemas de detecção de intrusão) e fornece uma trilha do histórico para acompanhamento pós-acidente. Registrar os seguintes eventos permite que uma empresa identifique e rastreie atividades potencialmente mal-intencionadas.
<b>10.2.1</b> Todos os acessos de usuários individuais aos dados do titular do cartão	<b>10.2.1</b> Verifique se todos os acessos individuais aos dados do titular do cartão estão registrados.	Indivíduos mal-intencionados poderiam tomar conhecimento de uma conta de usuário com acesso aos sistemas no CDE ou poderiam criar uma conta nova, não autorizada, para acessar os dados do titular do cartão. Um registro de todos os acessos individuais para os dados do titular do cartão pode identificar quais contas podem ter sido comprometidas ou usadas inadequadamente.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.2.2</b> Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos</p>	<p><b>10.2.2</b> Verifique se todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos são registradas.</p>	<p>Contas com privilégios maiores, como “administrador” ou “raiz”, têm o potencial para impactar fortemente a segurança ou a funcionalidade operacional de um sistema. Sem o registro das atividades executadas, uma empresa não é capaz de rastrear qualquer problema resultante de algum erro administrativo ou uso inadequado de privilégios em uma ação ou indivíduo específico.</p>
<p><b>10.2.3</b> Acesso a todas as trilhas de auditoria</p>	<p><b>10.2.3</b> Verifique se o acesso a todas as trilhas de auditoria é registrado.</p>	<p>Usuários mal-intencionados tentam frequentemente alterar os registros de auditoria para ocultar suas ações e um registro de acesso permite que uma empresa rastreie quaisquer inconsistências ou potenciais adulterações dos registros para uma conta individual. Ter acesso aos registros que identificam alterações, adições e exclusões pode ajudar a reconstituir os passos feitos pelo pessoal não autorizado.</p>
<p><b>10.2.4</b> Tentativas inválidas de acesso lógico</p>	<p><b>10.2.4</b> Verifique se as tentativas inválidas de acesso lógico estão registradas.</p>	<p>Indivíduos mal-intencionados na rede muitas vezes executam várias tentativas de acesso nos sistemas alvejados. Várias tentativas inválidas de logon podem ser um indicador de tentativas de um usuário não autorizado “forçar” ou adivinhar uma senha.</p>
<p><b>10.2.5</b> O uso e as alterações dos mecanismos de identificação e autenticação, inclusive, entre outros, a criação de novas contas, aumento de privilégios e demais alterações, adições ou exclusões de contas com privilégios raiz ou administrativos</p>	<p><b>10.2.5.a</b> Verifique se o uso dos mecanismos de identificação e autenticação é registrado.</p>	<p>Sem saber quem estava registrado no momento de um incidente, é impossível identificar as contas que possam ter sido usadas. Além disso, usuários mal-intencionados tentam manipular os controles de autenticação com o objetivo de contorná-los ou imitar uma conta válida.</p>
	<p><b>10.2.5.b</b> Verifique se todos os aumentos de privilégios são registrados.</p>	
	<p><b>10.2.5.c</b> Verifique se todas as alterações, adições ou exclusões em qualquer conta com privilégios raiz ou administrativos são registradas.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<b>10.2.6</b> Inicialização, interrupção ou pausa dos registros de auditoria	<b>10.2.6</b> Verifique se o que segue é registrado: <ul style="list-style-type: none"> <li>• Inicialização dos logs de auditoria</li> <li>• Interrupção ou pausa dos registros de auditoria.</li> </ul>	Desativar os logs de auditoria (ou pausá-los) antes de realizar atividades ilícitas é uma prática comum a usuários mal-intencionados que desejam evitar ser detectados. A inicialização dos logs de auditoria podem indicar que a função de registro foi desativada por um usuário para ocultar suas ações.
<b>10.2.7</b> Criação e exclusão de objetos do nível do sistema	<b>10.2.7</b> Verifique se a criação e a exclusão de objetos do nível do sistema são registrados.	Softwares mal-intencionados, como malwares, frequentemente criam ou substituem objetos no nível do sistema no sistema de destino para controlar uma função ou operação nesse sistema. Registrando quando os objetos do nível do sistema, como tabelas do banco de dados ou procedimentos armazenados, são criados ou excluídos, será mais fácil determinar se estas modificações foram autorizadas.
<b>10.3</b> Registre pelo menos as seguintes entradas de trilhas de auditoria para todos os componentes do sistema para cada evento:	<b>10.3</b> Por meio de entrevistas e da observação dos logs de auditoria, para cada evento auditável (no item 10.2), realize o seguinte:	Ao registrar esses detalhes para os eventos auditáveis em 10.2, um possível comprometimento poderá ser rapidamente identificado e com detalhes suficientes para saber quem, o que, onde, quando e como.
<b>10.3.1</b> Identificação do usuário	<b>10.3.1</b> Verifique se a identificação do usuário está incluída nas entradas do registro.	
<b>10.3.2</b> Tipo de evento	<b>10.3.2</b> Verifique se o tipo de evento está incluído nas entradas do registro.	
<b>10.3.3</b> Data e horário	<b>10.3.3</b> Verifique se a data e o horário estão incluídos nas entradas do registro.	
<b>10.3.4</b> Indicação de sucesso ou falha	<b>10.3.4</b> Verifique se a indicação de êxito ou falha está incluída nas entradas do registro.	
<b>10.3.5</b> Origem do evento	<b>10.3.5</b> Verifique se a origem do evento está incluída nas entradas do registro.	
<b>10.3.6</b> A identidade ou o nome dos dados afetados, componentes do sistema ou recurso.	<b>10.3.6</b> Verifique se a identidade ou o nome dos dados afetados, os componentes do sistema ou recursos estão incluídos nas entradas do registro.	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.4</b> Usando tecnologia de sincronização de tempo, sincronize todos os relógios e horários críticos do sistema e assegure-se de que os seguintes itens sejam implementados para adquirir, distribuir e armazenar horários.</p> <p><b>Observação:</b> <i>um exemplo de tecnologia de sincronização de horários é o Network Time Protocol (NTP).</i></p>	<p><b>10.4</b> Analise os processos e padrões de configuração para verificar se a tecnologia de sincronização de tempo está implementada e mantida atualizada pelos Requisitos 6.1 e 6.2 do PCI DSS.</p>	<p>A tecnologia para sincronização do horário é usada para sincronizar os relógios. Quando os relógios não são sincronizados adequadamente pode ser difícil, se não impossível, comparar arquivos de registro de diferentes sistemas e estabelecer uma sequência exata de eventos (cruciais para análise forense no caso de uma violação). Para equipes de forenses pós-incidente, a precisão e a consistência do horário ao longo de todos os sistemas e a hora de cada atividade são essenciais para determinar a forma como os sistemas foram comprometidos.</p>
<p><b>10.4.1</b> Sistemas críticos têm o horário correto e consistente.</p>	<p><b>10.4.1.a</b> Analise o processo para a aquisição, distribuição e armazenamento do horário correto na empresa para verificar se:</p> <ul style="list-style-type: none"> <li>• Apenas os servidores centrais de horário designados recebem sinais de horário de fontes externas e se os sinais de horário de fontes externas são baseadas no Tempo Atômico Internacional ou no UTC.</li> <li>• Onde houver mais de um servidor de horário designado, os servidores de horários se igualam um com o outro para manter a hora exata.</li> <li>• Os sistemas recebem informações de horário somente dos servidores centrais de horário designados.</li> </ul> <p><b>10.4.1.b</b> Observe as configurações dos parâmetros do sistema relacionadas ao horário para obter uma amostra dos componentes do sistema e verificar se:</p> <ul style="list-style-type: none"> <li>• Apenas os servidores centrais de horário designados recebem sinais de horário de fontes externas e se os sinais de horário de fontes externas são baseadas no Tempo Atômico Internacional ou no UTC.</li> <li>• Onde houver mais de um servidor de horário designado, os servidores centrais de horários designados se igualam um com o outro para manter a hora exata.</li> <li>• Os sistemas recebem o horário somente dos servidores centrais de horário designados.</li> </ul>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.4.2</b> Os dados de horário são protegidos.</p>	<p><b>10.4.2.a</b> Analise as definições de configuração e de sincronização de horário para verificar se o acesso aos dados de horário são restritos somente aos funcionários com necessidades comerciais de acesso aos dados de horário.</p> <p><b>10.4.2.b</b> Analise as definições, registros e processos de configuração e de sincronização de horário para verificar se qualquer alteração às definições de horário em sistemas críticos é registrada, monitorada e revisada.</p>	
<p><b>10.4.3</b> As definições de horário são recebidas de fontes de horário aceitas pelo setor.</p>	<p><b>10.4.3</b> Analise as configurações dos sistemas para verificar se os servidores de horário aceitam atualizações de fontes externas específicas, aceitas pelo setor (para evitar que um indivíduo mal-intencionado altere o relógio). Além disso, essas atualizações podem ser criptografadas com uma chave simétrica e as listas de controle de acesso podem ser criadas para especificar os endereços IP das máquinas clientes que serão fornecidas com as atualizações de horário (para evitar o uso não autorizado de servidores de horário internos).</p>	
<p><b>10.5</b> Proteja as trilhas de auditoria para que não possam ser alteradas.</p>	<p><b>10.5</b> Converse com os administradores do sistema e analise as configurações do sistema e permissões para verificar se as trilhas de auditoria estão protegidas de forma que não possam ser alteradas conforme segue:</p>	<p>Muitas vezes um indivíduo mal-intencionado que entra em uma rede tenta editar os logs de auditoria para ocultar suas atividades. Sem proteção adequada dos logs de auditoria, sua conclusão, precisão e integridade não poderão ser garantidas e os logs de auditoria poderão ser inutilizados como ferramenta de investigação após um comprometimento.</p>
<p><b>10.5.1</b> Limite a exibição de trilhas de auditoria às pessoas que têm uma necessidade relacionada à função.</p>	<p><b>10.5.1</b> Apenas os indivíduos que têm uma necessidade relacionada à função podem visualizar arquivos de trilha de auditoria.</p>	<p>Uma proteção adequada dos logs de auditoria inclui forte controle de acesso (limitar o acesso aos logs com base somente na “necessidade de divulgação”) e uso da separação física e da rede para deixar os logs mais difíceis de serem encontrados e modificados.</p>
<p><b>10.5.2</b> Proteja os arquivos de trilha de auditoria de modificações não autorizadas.</p>	<p><b>10.5.2</b> Os arquivos de trilha de auditoria atuais estão protegidos de modificações não autorizadas por meio de mecanismos de controle de acesso, separação física e/ou separação da rede.</p>	<p>Fazer imediatamente o backup dos logs para um servidor centralizado de log ou mídias que sejam difíceis de alterar mantém os registros protegidos mesmo se o sistema que gera os registros for comprometido.</p>
<p><b>10.5.3</b> Faça imediatamente o backup dos arquivos de trilha de auditoria em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.</p>	<p><b>10.5.3</b> Os arquivos de trilha de auditoria atuais têm o backup feito imediatamente em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.5.4</b> Documente registros quanto às tecnologias externas em um servidor de registros centralizado, seguro ou dispositivo de mídia.</p>	<p><b>10.5.4</b> Os registros quanto às tecnologias externas (por exemplo, sem fio, firewalls, DNS, e-mail) são escritos em um servidor de registro interno centralizado ou mídia seguros.</p>	<p>Ao gravar os logs de tecnologias que usam recursos externos, como sem fio, firewalls, DNS e servidores de e-mail, o risco de esses logs serem perdidos ou alterados é diminuído, pois eles estão mais seguros dentro da rede interna.</p> <p>Os logs podem ser escritos diretamente, ou transferidos ou copiados de sistemas externos para a mídia ou sistema interno seguros.</p>
<p><b>10.5.5</b> Use softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos logs para assegurar que os dados de registro existentes não possam ser alterados sem gerar alertas (embora os novos dados que estejam sendo adicionados não gerem um alerta).</p>	<p><b>10.5.5</b> Analise as configurações do sistema, os arquivos e resultados monitorados das atividades de monitoramento para verificar o uso de software para monitoramento da integridade do arquivo ou detecção de alterações nos registros.</p>	<p>Os sistemas de monitoramento da integridade do arquivo ou de detecção de alterações verificam as alterações nos arquivos críticos e notificam quando essas alterações são observadas. Para fins de monitoramento da integridade do arquivo, uma entidade normalmente monitora os arquivos que não mudam regularmente, mas que, quando alterados, indicam um possível comprometimento.</p>
<p><b>10.6</b> Revise os registros e ocorrências de segurança para todos os componentes do sistema para identificar irregularidades ou atividades suspeitas.</p> <p><b>Observação:</b> Ferramentas de coleta, análise e alerta dos logs podem ser usadas para atender a este requisito.</p>	<p><b>10.6</b> Realize as seguintes etapas:</p>	<p>Várias violações ocorrem durante dias ou meses antes de serem detectadas. Revisões regulares dos logs pelos funcionários ou meios automatizados podem identificar e resolver proativamente o acesso não autorizado ao ambiente de dados do titular do cartão.</p> <p>O processo de revisão do log não precisa ser manual. O uso de ferramentas de coleta, análise e alertas pode facilitar o processo identificando as ocorrências de logs que precisam ser revisados.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.6.1</b> Revise o que segue ao menos diariamente:</p> <ul style="list-style-type: none"> <li>• Todas as ocorrências de segurança</li> <li>• Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD</li> <li>• Logs de todos os componentes críticos do sistema</li> <li>• Registros de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do e-commerce, etc.).</li> </ul>	<p><b>10.6.1.a</b> Analise as políticas e os procedimentos de segurança para verificar se estão definidos para revisar o que segue, pelo menos diariamente, seja de forma manual ou por meio de ferramentas de logs:</p> <ul style="list-style-type: none"> <li>• Todas as ocorrências de segurança</li> <li>• Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD</li> <li>• Logs de todos os componentes críticos do sistema</li> <li>• Logs de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do comércio eletrônico, etc.)</li> </ul> <p><b>10.6.1.b</b> Observe os processos e questione os funcionários para verificar se o que segue é revisado, ao menos diariamente:</p> <ul style="list-style-type: none"> <li>• Todas as ocorrências de segurança</li> <li>• Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD</li> <li>• Logs de todos os componentes críticos do sistema</li> <li>• Registros de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do e-commerce, etc.).</li> </ul>	<p>A verificação diária dos logs minimiza a quantidade de tempo e exposição de uma violação em potencial.</p> <p>A revisão diária de ocorrências de segurança, por exemplo, avisos ou alertas que identificam atividades irregulares ou suspeitas, bem como registros dos componentes críticos do sistema e registros dos sistemas que desempenham funções de segurança, como firewalls, IDS/IPS, sistemas de monitoramento da integridade do arquivo (FIM), etc., é necessária para identificar possíveis problemas. Observe que a determinação de “ocorrência de segurança” varia para cada organização e pode considerar o tipo de tecnologia, local e função do dispositivo. As organizações também podem manter um parâmetro do tráfego “normal” para ajudar a identificar comportamentos irregulares.</p>
<p><b>10.6.2</b> Revise os logs de todos os outros componentes do sistema periodicamente com base nas políticas e estratégia de gerenciamento de risco da organização, conforme determinado pela avaliação de risco anual da organização.</p>	<p><b>10.6.2.a</b> Analise as políticas e os procedimentos de segurança para verificar se estão definidos procedimentos para revisar os logs de todos os outros componentes do sistema periodicamente, seja de forma manual ou por meio de ferramentas de logs, com base nas políticas e estratégia de gerenciamento de risco da organização.</p> <p><b>10.6.2.b</b> Analise a documentação da avaliação de risco da organização e questione os funcionários para verificar se as revisões são realizadas de acordo com as políticas e estratégia de gerenciamento de risco da organização.</p>	<p>Os logs para todos os outros componentes do sistema também devem ser revisados periodicamente para identificar indicações de possíveis problemas ou tentativas de obter acesso aos sistemas confidenciais por meio de sistemas menos confidenciais. A frequência de revisões deve ser determinada por uma avaliação de risco anual da entidade.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>10.6.3</b> Acompanhe as exceções e irregularidades identificadas durante o processo de revisão.</p>	<p><b>10.6.3.a</b> Analise as políticas e os procedimentos de segurança para verificar se estão definidos procedimentos para acompanhar as exceções e irregularidades identificadas durante o processo de revisão.</p> <p><b>10.6.3.b</b> Observe os processos e questione os funcionários para verificar se são realizados acompanhamentos das exceções e irregularidades.</p>	<p>Se as exceções e irregularidades identificadas durante o processo de revisão do registro não forem investigadas, a entidade pode não tomar conhecimento de atividades não autorizadas e potencialmente mal-intencionadas que estejam ocorrendo dentro de sua própria rede.</p>
<p><b>10.7</b> Mantenha um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, online, arquivado ou recuperável a partir do backup).</p>	<p><b>10.7.a</b> Analise as políticas e procedimentos de segurança para verificar se eles definem o que segue:</p> <ul style="list-style-type: none"> <li>• Políticas de manutenção de log de auditoria</li> <li>• Procedimentos para manter logs de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível online.</li> </ul> <p><b>10.7.b</b> Converse com os funcionários e analise os logs de auditoria para verificar se são armazenados por, pelo menos, um ano.</p> <p><b>10.7.c</b> Converse com os funcionários e observe os processos para verificar se os registros dos últimos três meses, pelo menos, encontram-se disponíveis para análise imediata.</p>	<p>Guardar os logs por pelo menos um ano leva em conta o fato de muitas vezes se levar um tempo até notar que ocorreu ou está ocorrendo um comprometimento e permite que os investigadores tenham um histórico de log suficiente para determinar melhor a quantidade de tempo de uma potencial violação e os possíveis sistemas afetados. Ao ter três meses de logs imediatamente disponíveis, uma entidade pode rapidamente identificar e minimizar o impacto da violação de dados. O armazenamento de logs em locais offline pode evitar que eles fiquem prontamente disponíveis, resultando em cronogramas mais longos para restaurar dados de log, executar análises e identificar sistemas ou dados afetados.</p>
<p><b>10.8 Requisito adicional, somente para prestadores de serviços:</b> Implementar processo para detecção e emissão de relatórios de falhas dos sistemas de controle de segurança crítica, inclusive, entre outros, falhas relacionadas a:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivírus</li> <li>• Controles de acesso físico</li> <li>• Controles de acesso lógico</li> </ul>	<p><b>10.8.a</b> Analise as políticas e procedimentos documentados para verificar se os processos são definidos para detecção em tempo hábil e emissão de relatórios de falhas dos sistemas de controle de segurança crítica, inclusive, entre outros, falhas relacionadas a:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivírus</li> <li>• Controles de acesso físico</li> <li>• Controles de acesso lógico</li> <li>• Mecanismos de registro de auditoria</li> <li>• Controles de segmentação (se usados)</li> </ul>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>Se não houver processos formais para detectar e alertar a ocorrência de falha nos controles de segurança crítica, as falhas podem passar despercebidas por períodos prolongados e conferir aos invasores tempo suficiente para comprometer sistemas e roubar dados confidenciais do ambiente de dados do titular de cartão.</p> <p>Os tipos específicos de falhas podem variar, a depender da função do dispositivo e da tecnologia</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<ul style="list-style-type: none"> <li>Mecanismos de registro de auditoria</li> <li>Controles de segmentação (se usados)</li> </ul> <p><i>Observação: Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i></p>	<p><b>10.8.b</b> Analise os processos de detecção e alerta e converse com os funcionários para verificar se há processos implementados para todos os controles de segurança crítica, e se a falha de um controle de segurança crítica resulta na geração de um alerta.</p>	<p>em uso. São exemplos de falhas comuns a interrupção na execução da função de segurança do sistema ou não funcionamento da forma pretendida; por exemplo, a exclusão de todas as regras do firewall ou firewall off-line.</p>
<p><b>10.8.1 Requisito adicional, somente para prestadores de serviços:</b> Solucionar falhas nos controles de segurança crítica em tempo hábil. Os processos para solucionar falhas nos controles de segurança devem incluir:</p> <ul style="list-style-type: none"> <li>Restabelecimento de funções de segurança</li> <li>Identificação e documentação da duração (data e hora do início ao fim) da falha de segurança</li> <li>Identificar e documentar as causas de falha, incluindo a causa raiz e documentar a correção necessária para tratar da causa raiz.</li> <li>Identificação e tratamento de quaisquer questões de segurança</li> </ul>	<p><b>10.8.1.a</b> Analise os procedimentos e as políticas documentadas e converse com o pessoal para verificar se há processos definidos e implementados para solucionar falhas no controle de segurança que incluam:</p> <ul style="list-style-type: none"> <li>Restabelecimento de funções de segurança</li> <li>Identificação e documentação da duração (data e hora do início ao fim) da falha de segurança</li> <li>Identificar e documentar as causas de falha, incluindo a causa raiz e documentar a correção necessária para tratar da causa raiz.</li> <li>Identificação e tratamento de quaisquer questões de segurança que surgiram durante a falha</li> <li>Proceder à avaliação de riscos para determinar a necessidade de outras ações como resultado da falha na segurança</li> <li>Implementação de controles para prevenir a causa da falha de reocorrer</li> <li>Retomar o monitoramento dos controles de segurança</li> </ul>	<p><i>Observação: Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</i></p> <p>Se os alertas referentes a falhas no controle de segurança crítica não são respondidos com agilidade e eficiência, os invasores podem aproveitar o tempo para inserção de software malicioso, controle sobre o sistema ou roubo de dados do ambiente da entidade.</p> <p>Evidências documentadas (p. ex., registros em um sistema de gerenciamento de problemas) devem conferir suporte para a existência de processos e procedimentos capazes de solucionar falhas de segurança. Além disso, o pessoal deve estar ciente de suas responsabilidades em caso de falha. Ações e respostas às falhas devem ser registradas nas</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>que surgiram durante a falha</p> <ul style="list-style-type: none"> <li>• Proceder à avaliação de riscos para determinar a necessidade de outras ações como resultado da falha na segurança</li> <li>• Implementação de controles para prevenir a causa da falha de reocorrer</li> <li>• Retomar o monitoramento dos controles de segurança</li> </ul> <p><b>Observação:</b> Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</p>	<p><b>10.8.1.b</b> Analise os registros para verificar se as falhas no controle de segurança estão documentadas e incluem:</p> <ul style="list-style-type: none"> <li>• Identificação das causas da falha, incluindo a causa raiz</li> <li>• Duração (data e hora de início e fim) da falha de segurança</li> <li>• Detalhes da correção necessária para solucionar a causa raiz</li> </ul>	<p>evidências documentadas.</p>
<p><b>10.9</b> Certifique-se de que as políticas de segurança e os procedimentos operacionais para monitoramento de todos os acessos aos recursos da rede e aos dados do titular do cartão estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>10.9</b> Analise a documentação e converse com os funcionários para verificar se as políticas de segurança e os procedimentos operacionais para monitoramento de todos os acessos aos recursos da rede e aos dados do titular do cartão estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais diários para monitorar todos os acessos aos recursos de rede e dados do titular do cartão continuamente.</p>

**Requisito 11: Testar regularmente os sistemas e processos de segurança.**

As vulnerabilidades estão sendo continuamente descobertas por indivíduos mal-intencionados e pesquisadores e são apresentadas por novos softwares. Os componentes do sistema, processos e softwares personalizados devem ser testados com frequência para assegurar que os controles de segurança continuem refletindo um ambiente em transformação.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>11.1</b> Implemente processos para testar a presença de pontos de acesso sem fio (802.11) e detectar e identificar todos os pontos de acesso sem fio autorizados e não autorizados trimestralmente.</p> <p><b>Observação:</b> Métodos que podem ser usados no processo incluem, entre outros, varreduras de rede sem fio, inspeções físicas/virtuais de componentes e infraestrutura do sistema, controle de acesso à rede (NAC) ou IDS/IPS sem fio. Qualquer método usado deve ser suficiente para detectar e identificar dispositivos autorizados e não autorizados.</p>	<p><b>11.1.a</b> Analise as políticas e procedimentos para verificar se estão definidos processos para detectar e identificar pontos de acesso sem fio autorizados e não autorizados trimestralmente.</p>	<p>A implementação e/ou exploração da tecnologia sem fio dentro de uma rede é um dos caminhos mais comuns para usuários mal-intencionados obterem acesso à rede e aos dados do titular do cartão. Se um dispositivo sem fio ou uma rede forem instalados sem o conhecimento da empresa, ele pode permitir que um invasor entre na rede de forma fácil e invisível. Dispositivos sem fio não autorizados devem ser ocultados ou anexados a um computador ou outro componente do sistema, ou ser anexados diretamente a uma porta ou dispositivo da rede, como um switch ou roteador. Qualquer desses dispositivos não autorizados podem resultar em um ponto não autorizado de acesso ao ambiente.</p> <p>Saber quais dispositivos sem fio são autorizados pode ajudar os administradores a identificar mais rapidamente os dispositivos sem fio não autorizados e reagir à identificação de pontos de acesso sem fio não autorizados ajuda a minimizar proativamente a exposição do CDE a indivíduos mal-intencionados.</p> <p>Em função da facilidade com que o ponto de acesso sem fio pode ser conectado a uma rede, da dificuldade em detectar sua presença e do risco cada vez maior apresentado por dispositivos sem fio não autorizados, esses processos devem ser executados até quando existir uma política proibindo o uso da tecnologia sem fio.</p> <p>O tamanho e a complexidade de um ambiente privado determinarão as ferramentas e os processos adequados a serem usados para</p>
	<p><b>11.1.b</b> Verifique se a metodologia é adequada para detectar e identificar qualquer ponto de acesso sem fio não autorizado, incluindo ao menos o seguinte:</p> <ul style="list-style-type: none"> <li>• Cartões WLAN inseridos nos componentes do sistema</li> <li>• Dispositivos móveis ou portáteis fixados a componentes do sistema para criar um ponto de acesso sem fio (por exemplo, por USB, etc.)</li> <li>• Dispositivos sem fio conectados a uma porta de rede ou a um dispositivo de rede.</li> </ul>	
	<p><b>11.1.c</b> Se for realizada a varredura sem fio, analise os resultados das varreduras sem fio recentes para verificar se:</p> <ul style="list-style-type: none"> <li>• Os pontos de acesso sem fio autorizados e não autorizados estão identificados, e</li> <li>• A varredura é realizada ao menos trimestralmente para todas as instalações e componentes do sistema.</li> </ul>	
	<p><b>11.1.d</b> Se o monitoramento automatizado for utilizado (por exemplo, IDS/IPS sem fio, NAC, etc.), verifique que a configuração gerará alertas para avisar os funcionários.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
		fornecer garantia suficiente de que um ponto de acesso sem fio intruso não tenha sido instalado no ambiente.
<p><b>11.1.1</b> Mantenha um inventário de pontos de acesso sem fio autorizados incluindo uma justificativa comercial documentada.</p>	<p><b>11.1.1</b> Analise os registros documentados para verificar se é mantido um inventário de pontos de acesso sem fio autorizados e se uma justificativa comercial está documentada para todos os pontos de acesso sem fio autorizados.</p>	<p><b>Por exemplo:</b> No caso de um único quiosque de revenda autônomo em um shopping, onde todos os componentes de comunicação estão contidos em estojos antiadulteração e indicadores de adulteração, executando inspeções físicas detalhadas no próprio quiosque pode ser suficiente para fornecer garantias de que nenhum ponto de acesso sem fio intruso foi anexado ou instalado. No entanto, em um ambiente com vários nós (como em uma grande loja de revenda, uma central de atendimento, sala de servidor ou centro de dados), a inspeção física detalhada é difícil. Nesse caso, vários métodos podem ser combinados para atender ao requisito, como executar inspeções físicas no sistema em conjunto com os resultados de um analisador sem fio.</p>
<p><b>11.1.2</b> Implemente procedimentos de resposta a incidentes para o caso de serem detectados pontos de acesso sem fio não autorizados.</p>	<p><b>11.1.2.a</b> Analise o plano de resposta a incidentes da organização (Requisito 12.10) para verificar se ele define e exige uma reação no caso de ser detectado um ponto de acesso sem fio não autorizado.</p> <p><b>11.1.2.b</b> Converse com os funcionários responsáveis e/ou inspecione as varreduras sem fio recentes e as respostas relacionadas para verificar se a ação é realizada quando pontos de acesso sem fio não autorizados são encontrados.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>11.2</b> Execute varreduras quanto às vulnerabilidades das redes internas e externas pelo menos trimestralmente e após qualquer mudança significativa na rede (como instalações de novos componentes do sistema, mudanças na topologia da rede, modificações das normas do firewall, aprimoramentos de produtos).</p> <p><b>Observação:</b> <i>vários relatórios de varredura podem ser combinados no processo de varredura trimestral para mostrar que todos os sistemas foram mapeados e que todas as vulnerabilidades aplicáveis foram resolvidas. Pode ser exigida uma documentação adicional para verificar se as vulnerabilidades não resolvidas estão em processo de serem solucionadas.</i></p> <p><i>Para a conformidade inicial com o PCI DSS, não é necessário que as quatro varreduras trimestrais aprovadas sejam concluídas se o assessor verificar que 1) o resultado da varredura mais recente foi uma varredura aprovada, 2) a entidade possui políticas e procedimentos documentados que requerem a sequência de varreduras trimestrais e 3) as vulnerabilidades observadas nos resultados da varredura tenham sido corrigidas conforme mostrado em uma nova varredura. Nos anos seguintes após a análise inicial do PCI DSS, quatro varreduras trimestrais aprovadas devem ter ocorrido.</i></p>	<p><b>11.2</b> Analise os relatórios de varredura e documentação de suporte para verificar se as varreduras de vulnerabilidades internas e externas são realizadas conforme segue:</p>	<p>Varredura de vulnerabilidade é a combinação entre métodos, técnicas e/ou ferramentas automatizadas ou manuais executada em servidores e dispositivos da rede interna e externa, com o objetivo de expor possíveis vulnerabilidades que possam ser encontradas e exploradas por indivíduos mal-intencionados.</p> <p>Há três tipos de varredura de vulnerabilidades exigidas para o PCI DSS:</p> <ul style="list-style-type: none"> <li>• Varredura interna de vulnerabilidades trimestral feita por funcionários qualificados (o uso de um Fornecedor de Varredura Aprovado (ASV) para o PCI SSC não é necessário)</li> <li>• Varredura externa de vulnerabilidades trimestral, a qual deve ser realizada por um ASV</li> <li>• Varredura interna e externa conforme necessário após mudanças significativas</li> </ul> <p>Quando esses pontos fracos são identificados, a entidade os corrige e repete a varredura até que todas as vulnerabilidades tenham sido corrigidas.</p> <p>Identificar e resolver as vulnerabilidades em tempo hábil reduz as chances de exploração de uma vulnerabilidade e o comprometimento potencial de um componente do sistema ou de dados do titular do cartão.</p>
<p><b>11.2.1</b> Realizar varreduras para verificação de vulnerabilidade interna trimestralmente. Solucionar</p>	<p><b>11.2.1.a</b> Analise os relatórios de varredura e verifique se ocorreram quatro varreduras internas trimestrais nos últimos 12 meses.</p>	<p>Um processo estabelecido para identificar vulnerabilidades em sistemas internos exige que as varreduras de vulnerabilidade sejam</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>vulnerabilidades e executar novas varreduras para verificar se todas as vulnerabilidades de “alto risco” foram resolvidas de acordo com a classificação de vulnerabilidades da entidade (conforme Requisito 6.1). As varreduras devem ser realizadas por uma equipe qualificada.</p>	<p><b>11.2.1.b</b> Analise os relatórios de varredura e verifique se todas as vulnerabilidades de “alto risco” foram solucionadas e se o processo de varredura inclui novas varreduras para verificar se as vulnerabilidades de “alto risco” (conforme definidas no Requisito 6.1 do PCI DSS) foram solucionadas.</p> <p><b>11.2.1.c</b> Converse com os funcionários para verificar se a varredura foi realizada por um recurso interno qualificado ou um terceiro externo qualificado e, caso seja aplicável, se há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV).</p>	<p>conduzidas trimestralmente. As vulnerabilidades que representam o maior risco ao ambiente (por exemplo, classificadas como “Alto” pelo requisito 6.1) deve ser resolvida com a maior prioridade.</p> <p>Varreduras de vulnerabilidade internas podem ser realizadas por profissionais internos e qualificados que sejam razoavelmente independentes dos componentes do sistema que estão sendo mapeados (por exemplo, um administrador de firewall não deve ser responsável pela varredura do firewall), ou a entidade pode optar por fazer as varreduras de vulnerabilidade internas por uma empresa especializada em varreduras de vulnerabilidade.</p>
<p><b>11.2.2</b> Realize varreduras externas trimestrais de vulnerabilidades por meio de um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da Indústria de cartões de pagamento (PCI SSC). Realiza novas varreduras conforme necessário, até que se chegue a varreduras aprovadas.</p> <p><b>Observação:</b> as varreduras externas trimestrais de vulnerabilidades devem ser realizadas por um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da indústria de cartões de pagamento (PCI SSC).</p> <p>Consulte o Guia do programa ASV publicado no site do PCI SSC para saber sobre responsabilidades de varredura do cliente, preparação de varredura, etc.</p>	<p><b>11.2.2.a</b> Revise o resultado das varreduras externas de vulnerabilidades dos quatro últimos trimestres e verifique se ocorreram quatro varreduras nos últimos 12 meses.</p> <p><b>11.2.2.b</b> Analise os resultados de cada varredura trimestral e de novas varreduras para verificar se elas atendem aos requisitos do Guia do programa ASV (por exemplo, nenhuma vulnerabilidade classificada com mais de 4.0 pelo CVSS e sem falhas automáticas).</p> <p><b>11.2.2.c</b> Revise os relatórios de varredura para verificar se as varreduras foram concluídas por um Fornecedor de Varredura Aprovado (ASV) pelo PCI SSC.</p>	<p>Como redes externas têm um risco maior de comprometimento, a varredura de vulnerabilidade externa trimestral deve ser realizada por um Fornecedor de Varreduras Aprovado (ASV) do PCI SSC.</p> <p>Um programa de varredura robusto garante que as varreduras sejam executadas e as vulnerabilidades solucionadas em tempo hábil.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>11.2.3</b> Realize varreduras internas e externas e novas varreduras se necessário, após qualquer mudança significativa. As varreduras devem ser realizadas por uma equipe qualificada.</p>	<p><b>11.2.3.a</b> Inspeccione correlacione a documentação do controle de alterações e realize uma varredura nos relatórios para verificar se os componentes do sistema sujeitos a qualquer alteração significativa passaram por varredura.</p>	<p>A determinação do que constitui uma alteração “significativa” depende muito da configuração de um determinado ambiente. Se uma melhoria ou modificação puder permitir o acesso aos dados do titular do cartão ou afetar a segurança do ambiente de dados do titular do cartão, ela pode ser considerada significativa.</p> <p>Mapear um ambiente depois de qualquer alteração significativa ter sido feita garante que todas as alterações foram concluídas adequadamente para que a segurança do ambiente não tenha sido comprometida como resultado da alteração. Todos os componentes do sistema afetados pela alteração precisam passar por varredura.</p>
	<p><b>11.2.3.b</b> Analise os relatórios de varredura e verifique se o processo inclui novas varreduras até que:</p> <ul style="list-style-type: none"> <li>• Não existam varreduras com pontuação maior do que 4.0 pelo CVSS para varreduras externas.</li> <li>• Todas as vulnerabilidades de “alto risco”, conforme definidas no Requisito 6.1 do PCI DSS, estejam solucionadas para varreduras internas.</li> </ul>	
	<p><b>11.2.3.c</b> Verifique se a varredura foi realizada por um recurso interno qualificado ou um terceiro externo qualificado e, caso seja aplicável, se há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV).</p>	
<p><b>11.3</b> Implemente uma metodologia para testes de penetração que inclua o seguinte:</p> <ul style="list-style-type: none"> <li>• É baseada nas abordagens de testes de penetração aceitas pelo setor (por exemplo, NIST SP800-115)</li> <li>• Abrange todo o perímetro do CDE e sistemas críticos</li> <li>• Inclui testes de dentro e fora da rede</li> <li>• Inclui testes para validar qualquer controle de redução no escopo e segmentação</li> <li>• Define testes de penetração da camada do aplicativo para incluir, pelo menos, as vulnerabilidades listadas no requisito 6.5</li> <li>• Define testes de penetração da camada da rede que incluam</li> </ul>	<p><b>11.3</b> Analise a metodologia de testes de penetração e questione o funcionário responsável para verificar se está implementada uma metodologia que inclua o seguinte:</p> <ul style="list-style-type: none"> <li>• É baseada nas abordagens de testes de penetração aceitas pelo setor (por exemplo, NIST SP800-115)</li> <li>• Abrange todo o perímetro do CDE e sistemas críticos</li> <li>• Testes de dentro e fora da rede</li> <li>• Inclui testes para validar qualquer controle de redução no escopo e segmentação</li> <li>• Define testes de penetração da camada do aplicativo para incluir, pelo menos, as vulnerabilidades listadas no requisito 6.5</li> <li>• Define testes de penetração da camada da rede que incluam componentes compatíveis com as funções da rede e com os sistemas operacionais</li> <li>• Inclui revisão e consideração de ameaças e vulnerabilidades ocorridas nos últimos 12 meses</li> </ul>	<p>O objetivo de um teste de penetração é estimular uma situação de invasão real com o objetivo de identificar até onde um invasor conseguiria penetrar em um ambiente. Isso permite que a entidade tenha mais compreensão sobre sua potencial exposição e desenvolva uma estratégia para se defender de invasões.</p> <p>Um teste de penetração difere de uma varredura de vulnerabilidade, uma vez que o teste de penetração é um processo ativo que pode incluir a exploração de vulnerabilidades identificadas. Conduzir uma varredura de vulnerabilidade pode ser um dos primeiros passos que um testador de penetração realizará para planejar uma estratégia de teste, mesmo que não seja o único passo. Mesmo que uma varredura de vulnerabilidade não detecte nenhuma vulnerabilidade conhecida, o testador de penetração irá normalmente tomar</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>componentes compatíveis com as funções da rede e com os sistemas operacionais</p> <ul style="list-style-type: none"> <li>Inclui revisão e consideração de ameaças e vulnerabilidades ocorridas nos últimos 12 meses</li> <li>Especifica a conservação dos resultados de testes de penetração e resultados de atividades de reparo.</li> </ul>	<ul style="list-style-type: none"> <li>Especifica a conservação dos resultados de testes de penetração e resultados de atividades de reparo.</li> </ul>	<p>conhecimento suficiente sobre o sistema para identificar possíveis lacunas de segurança.</p> <p>O teste de penetração é geralmente um processo altamente manual. Enquanto algumas ferramentas automatizadas podem ser usadas, o testador utiliza seu conhecimento de sistemas para penetrar em um ambiente. Normalmente o testador irá conectar diversos tipos de explorações com o objetivo de ultrapassar camadas de defesas. Por exemplo, se o testador encontrar meios de obter acesso a um servidor de aplicativo, em seguida ele usará o servidor comprometido como um ponto de preparação para uma nova invasão com base nos recursos a que o servidor tem acesso. Dessa forma, o testador é capaz de simular os métodos utilizados por um invasor para identificar áreas de fraquezas potenciais no ambiente.</p> <p><i>As técnicas de teste de penetração serão diferentes para diferentes organizações e o tipo, profundidade e complexidade do teste dependerá do ambiente específico e da avaliação de risco da organização.</i></p>
<p><b>11.3.1</b> Realize <i>testes de penetração</i> externos pelo menos uma vez ao ano e após qualquer melhoria ou modificação significativa na infraestrutura ou nos aplicativos (como uma melhoria no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor Web adicionado ao ambiente).</p>	<p><b>11.3.1.a</b> Analise o escopo do trabalho e os resultados do teste de penetração mais recente para verificar se os testes de penetração são realizados conforme segue:</p> <ul style="list-style-type: none"> <li>De acordo com a metodologia definida</li> <li>Pelo menos uma vez ao ano</li> <li>Após quaisquer alterações significativas no ambiente.</li> </ul> <p><b>11.3.1.b</b> Verifique se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e, caso seja aplicável, se há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV).</p>	<p>O teste de penetração conduzido regularmente e após mudanças significativas no ambiente é uma medida de segurança proativa que ajuda a minimizar o possível acesso ao CDE por indivíduos mal-intencionados.</p> <p>A determinação do que constitui uma melhoria ou modificação significativa depende muito da configuração de um determinado ambiente. Se uma melhoria ou modificação puder permitir o acesso aos dados do titular do cartão ou afetar a segurança do ambiente de dados do titular do cartão, ela pode ser considerada significativa. Realizar testes de penetração após melhorias e modificações da rede garante que os controles supostamente implementados ainda estejam</p>
<p><b>11.3.2</b> Realize <i>testes de penetração</i> internos pelo menos uma vez ao ano e</p>	<p><b>11.3.2.a</b> Analise o escopo do trabalho e os resultados do teste de penetração mais recente para verificar se os testes</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>após qualquer melhoria ou modificação significativa na infraestrutura ou nos aplicativos (como uma melhoria no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor Web adicionado ao ambiente).</p>	<p>de penetração são realizados conforme a seguir.</p> <ul style="list-style-type: none"> <li>• De acordo com a metodologia definida</li> <li>• Pelo menos uma vez ao ano</li> <li>• Após quaisquer alterações significativas no ambiente.</li> </ul>	<p>funcionando efetivamente após a melhoria ou modificação.</p>
	<p><b>11.3.2.b</b> Verifique se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e, caso seja aplicável, se há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV).</p>	
<p><b>11.3.3</b> As vulnerabilidades exploráveis encontradas durante o teste de penetração são corrigidas e o teste é repetido para verificar as correções.</p>	<p><b>11.3.3</b> Analise os resultados do teste de penetração para verificar se as vulnerabilidades exploráveis observadas foram corrigidas e se o teste repetido confirmou que ela foi corrigida.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>11.3.4</b> Se for utilizada a segmentação para isolar o CDE de outras redes, realize testes de penetração, ao menos, uma vez por ano e após qualquer alteração nos métodos/controles de segmentação, para verificar se os métodos de segmentação são operacionais e eficientes, e se isolam todos os sistemas fora do escopo dos sistemas no CDE.</p>	<p><b>11.3.4.a</b> Analise os controles de segmentação e revise a metodologia de teste de penetração para verificar se os procedimentos do teste são definidos para testar todos os métodos de segmentação, com o objetivo de confirmar se são operacionais e eficientes, e isole todos os sistemas fora do escopo dos sistemas no CDE.</p> <p><b>11.3.4.b</b> Analise os resultados do teste de penetração mais recente para verificar se:</p> <ul style="list-style-type: none"> <li>• O teste de penetração para verificação dos controles de segmentação é executado, pelo menos, uma vez ao ano e após qualquer mudança nos métodos/controles da segmentação.</li> <li>• Os testes de penetração abrangem todos os controles/métodos de segmentação em uso.</li> <li>• Os testes de penetração verificam se os controles/métodos de segmentação são operacionais e eficientes, e se isolam todos os sistemas fora de escopo dos sistemas no CDE.</li> </ul> <p><b>11.3.4.c</b> Verifique se o teste foi realizado por um recurso interno qualificado ou terceiro externo qualificado e, quando aplicável, se há independência organizacional em relação ao responsável pelo teste (desnecessário que seja QSA ou ASV).</p>	<p>O teste de penetração é uma ferramenta importante para confirmar se qualquer segmentação implantada para isolar o CDE de outras redes é efetiva. O teste de penetração deve focar nos controles da segmentação, tanto de dentro quanto de fora da rede da entidade, mas fora do CDE, para confirmar que eles não podem passar pelos controles da segmentação para acessar o CDE. Por exemplo, teste de rede e/ou varredura para portas abertas, para verificar se não há nenhuma conectividade entre as redes de fora e dentro do escopo.</p>
<p><b>11.3.4.1 Requisito adicional, somente para prestadores de serviços:</b> Se a segmentação for utilizada, confirme o escopo do PCI DSS por meio do teste de penetração nos controles de segmentação, pelo menos, semestralmente e após quaisquer alterações aos controles/métodos de segmentação.</p> <p><b>Observação:</b> Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</p>	<p><b>11.3.4.1.a</b> Analise os resultados do teste de penetração mais recente para verificar se:</p> <ul style="list-style-type: none"> <li>• O teste de penetração para verificação dos controles de segmentação é executado, pelo menos, semestralmente e após qualquer mudança nos métodos/controles da segmentação.</li> <li>• Os testes de penetração abrangem todos os controles/métodos de segmentação em uso.</li> <li>• Os testes de penetração verificam se os controles/métodos de segmentação são operacionais e eficientes, e se isolam todos os sistemas fora de escopo dos sistemas no CDE.</li> </ul>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>Para prestadores de serviços, a validação do escopo do PCI DSS deve ser executada sempre que possível, para garantir que o escopo do PCI DSS permaneça atualizado e alinhado às mudanças nos objetivos comerciais.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>11.3.4.1.b</b> Verifique se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e, quando aplicável, se há independência organizacional em relação ao responsável pelo teste (desnecessário que seja QSA ou ASV).</p>	
<p><b>11.4</b> Use técnicas de detecção de invasão e/ou prevenção contra invasões para detectar e/ou evitar invasões na rede. Monitore todo o tráfego no perímetro do ambiente de dados do titular do cartão, bem como nos pontos críticos do ambiente e alerte as equipes sobre comprometimentos suspeitos.</p> <p>Mantenha todos os mecanismos de detecção e prevenção contra invasões, diretrizes e assinaturas atualizados.</p>	<p><b>11.4.a</b> Analise as configurações do sistema e diagramas da rede para verificar se as técnicas (como sistemas de detecção e/ou prevenção contra invasões) estão implementadas para monitorar todo o tráfego:</p> <ul style="list-style-type: none"> <li>No perímetro do ambiente dos dados do titular do cartão</li> <li>Nos pontos críticos do ambiente dos dados do titular do cartão.</li> </ul> <p><b>11.4.b</b> Analise as configurações do sistema e questione os funcionários responsáveis para confirmar se as técnicas de detecção e/ou prevenção contra invasão alertam os funcionários de comprometimentos suspeitos.</p> <p><b>11.4.c</b> Analise as configurações de IDS/IPS e a documentação do fornecedor para verificar se as técnicas de detecção e/ou prevenção contra invasão estão configuradas, mantidas e atualizadas de acordo com as instruções do fornecedor para assegurar uma proteção ideal.</p>	<p>As técnicas de detecção e/ou prevenção contra invasões (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, trojans e outros tipos de malware) e envia alertas e/ou interrompe a tentativa enquanto ela está acontecendo. Sem uma abordagem proativa a uma detecção de atividade não autorizada, invasões (ou mau uso) de recursos de computador podem passar despercebidas em tempo real. Os alertas de segurança gerados por essas técnicas devem ser monitorados, de forma que as tentativas de invasão possam ser interrompidas.</p>
<p><b>11.5</b> Implemente um mecanismo de detecção de mudanças (por exemplo, ferramentas de monitoramento da integridade do arquivo) para alertar a equipe sobre modificações não autorizadas (inclusive alterações, acréscimos e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configure o software para executar comparações de arquivos críticos, pelo menos, uma vez por semana.</p> <p><i>(Continua na próxima página)</i></p>	<p><b>11.5.a</b> Verifique o uso de um mecanismo de detecção de mudanças observando as configurações do sistema e os arquivos monitorados, bem como analisando os resultados das atividades de monitoramento.</p> <p>Exemplos de arquivos que devem ser monitorados:</p> <ul style="list-style-type: none"> <li>Executáveis do sistema</li> <li>Executáveis dos aplicativos</li> <li>Arquivos de configuração e parâmetro</li> <li>Arquivos de log e auditoria, históricos ou arquivados, armazenados centralmente</li> <li>Arquivos críticos adicionais determinados pela entidade (por exemplo, por meio de avaliação de risco ou outros meios).</li> </ul>	<p>As soluções em detecção de mudanças, como ferramentas de monitoramento da integridade do arquivo (FIM), verificam alterações, acréscimos e exclusões de arquivos críticos, bem como notificam quando as mudanças são detectadas. Se não implementadas corretamente e se o resultado da solução de detecção de mudanças não for monitorado, um indivíduo mal-intencionado pode adicionar, remover ou alterar conteúdos do arquivo de configuração, programas do sistema operacional ou executáveis dos aplicativos. Alterações não autorizadas, se não detectadas, podem tornar os controles de segurança ineficazes e/ou resultar no roubo dos dados do titular do</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>Observação:</b> Para fins de detecção de alterações, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Os mecanismos de detecção de alterações, como produtos de monitoramento da integridade dos arquivos, normalmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para os aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).</p>	<p><b>11.5.b</b> Verifique se o mecanismo está configurado para alertar funcionários sobre modificações não autorizadas (inclusive alterações, acréscimos e exclusões) de arquivos críticos e para realizar comparações de arquivos críticos, ao menos, uma vez por semana.</p>	<p>cartão sem impacto perceptível no processamento normal.</p>
<p><b>11.5.1</b> Implemente um processo para responder a qualquer alerta gerado pela solução de detecção de alterações.</p>	<p><b>11.5.1</b> Converse com os funcionários para verificar se todos os alertas são investigados e resolvidos.</p>	
<p><b>11.6</b> Certifique-se de que as políticas de segurança e procedimentos operacionais para o teste e monitoramento da segurança estejam documentados, em uso e conhecidos por todas as partes envolvidas.</p>	<p><b>11.6</b> Analise a documentação e converse com os funcionários para verificar se as políticas de segurança e os procedimentos operacionais para teste e monitoramento da segurança estão:</p> <ul style="list-style-type: none"> <li>• Documentados,</li> <li>• Em uso, e</li> <li>• Conhecidos por todas as partes envolvidas.</li> </ul>	<p>Os funcionários precisam estar cientes e seguir as políticas de segurança e os procedimentos operacionais para monitorar e testar a segurança continuamente.</p>

## Manter uma política de segurança de informações

### **Requisito 12: Mantenha uma política que aborde a segurança da informação para todas as equipes.**

Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles. Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los. Para as finalidades do Requisito 12, “funcionário” refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias e prestadores de serviços e consultores que “residem” no endereço da entidade ou têm acesso ao ambiente de dados do titular do cartão.

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<b>12.1</b> Defina, publique, mantenha e dissemine uma política de segurança.	<b>12.1</b> Analise a política de segurança da informação e verifique se a política foi publicada e disseminada a todos os funcionários relevantes (incluindo fornecedores e parceiros comerciais).	A política de segurança de informações de uma empresa cria um guia para implementar as medidas de segurança para proteger seus ativos mais valiosos. Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los.
<b>12.1.1</b> Revise a política de segurança ao menos uma vez por ano e atualize a política quando o ambiente for alterado.	<b>12.1.1</b> Verifique se a política de segurança da informação é analisada pelo menos uma vez por ano e atualizada conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente de risco.	As ameaças de segurança e os métodos de proteção evoluem rapidamente. Sem atualizar a política de segurança para refletir essas alterações, agora são abordadas novas medidas de proteção para lutar contra essas ameaças.
<b>12.2</b> Implemente um processo de avaliação de risco que: <ul style="list-style-type: none"> <li>Seja realizado ao menos uma vez por ano e quando houver modificações significativas no ambiente (por exemplo,</li> </ul>	<b>12.2.a</b> Verifique se há um processo de avaliação de risco documentado que: <ul style="list-style-type: none"> <li>Identifique os recursos, ameaças e vulnerabilidades críticas</li> <li>Resulte em uma análise formal e documentada de risco</li> </ul>	Uma avaliação de riscos permite a uma organização identificar ameaças e vulnerabilidades relacionadas que têm o potencial de causar um impacto negativo em seus negócios. Exemplos de diferentes

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>aquisição, fusão, transferência, etc.),</p> <ul style="list-style-type: none"> <li>Identifique os recursos, ameaças e vulnerabilidades críticos, e</li> <li>Resulte em uma análise formal e documentada de risco.</li> </ul> <p><i>Os exemplos de metodologias de avaliação de risco incluem, entre outros, OCTAVE, ISO 27005 e NIST SP 800-30.</i></p>	<p><b>12.2.b</b> Analise a documentação da avaliação de risco para verificar se o processo de avaliação de risco é realizada ao menos uma vez por ano e quando houver alterações significativas no ambiente.</p>	<p>considerações de risco incluem crime cibernético, ataques à web e malware em POS. Os recursos podem então ser alocados com eficácia para implementar controles que reduzem a probabilidade e/ou o impacto potencial da ameaça em questão.</p> <p>Realizar avaliações de riscos anuais e quando houver alterações significativas permite à organização manter-se atualizada com as mudanças organizacionais e ameaças, tendências e tecnologias em evolução.</p>
<p><b>12.3</b> Desenvolva o uso de políticas de tecnologias críticas e defina o uso apropriado destas tecnologias.</p> <p><i>Observação: exemplos de tecnologias críticas incluem, entre outros, tecnologias de acesso remoto e sem fio, laptops, tablets, mídia eletrônica removível, uso de e-mails e da internet.</i></p> <p>Garanta que essas políticas de utilização exijam o seguinte:</p>	<p><b>12.3</b> Analise as políticas de uso das tecnologias críticas e questione os funcionários responsáveis para verificar se as seguintes políticas estão implementadas e são seguidas:</p>	<p>As políticas de uso por funcionários podem proibir o uso de determinados dispositivos e outras tecnologias, se for essa a política da empresa, ou fornecer orientação para os funcionários quanto ao uso e à implementação corretos. Se políticas de uso não estiverem vigentes, os funcionários podem usar as tecnologias na violação da política da empresa, permitindo que indivíduos mal-intencionados consigam acesso a sistemas críticos e dados do titular do cartão.</p>
<p><b>12.3.1</b> Aprovação explícita por partes autorizadas</p>	<p><b>12.3.1</b> Verifique se as políticas de utilização incluem processos para aprovação explícita das partes autorizadas para usar as tecnologias.</p>	<p>Sem exigir aprovação adequada do gerenciamento para implementação dessas tecnologias, um funcionário pode implementar inocentemente uma solução para uma necessidade de negócios percebida, mas também abrir um grande buraco que deixe os sistemas e dados críticos vulneráveis a indivíduos mal-intencionados.</p>
<p><b>12.3.2</b> Autenticação para o uso da tecnologia</p>	<p><b>12.3.2</b> Verifique se as políticas de utilização incluem processos para que todo o uso da tecnologia seja autenticado com ID de usuário e senha ou outro item de autenticação (por exemplo, token).</p>	<p>Se a tecnologia for implementada sem autenticação adequada (IDs de usuário e senhas, tokens, VPNs, etc.), indivíduos mal-intencionados podem facilmente usar essa tecnologia desprotegida para acessar sistemas críticos e dados do titular do cartão.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.3.3</b> Uma lista de todos esses dispositivos e equipes com acesso</p>	<p><b>12.3.3</b> Verificar se o uso das políticas define:</p> <ul style="list-style-type: none"> <li>• Uma lista de todos os dispositivos críticos e</li> <li>• Uma lista de pessoas autorizadas a usar os dispositivos.</li> </ul>	<p>Os indivíduos mal-intencionados podem violar a segurança física e colocar seus próprios dispositivos na rede como uma “backdoor”. Os funcionários também podem se desviar dos procedimentos e instalar dispositivos. Um inventário preciso, com rótulos adequados nos dispositivos, permite uma rápida identificação das instalações não aprovadas.</p>
<p><b>12.3.4</b> Um método para determinar prontamente e precisamente o proprietário, informações de contato e propósito (por exemplo, etiqueta, codificação, e/ou inventário de dispositivos)</p>	<p><b>12.3.4</b> Verifique se as políticas de utilização definem um método para determinar prontamente e precisamente o proprietário, informações de contato e propósito (por exemplo, etiqueta, codificação, e/ou inventário de dispositivos).</p>	<p>Os indivíduos mal-intencionados podem violar a segurança física e colocar seus próprios dispositivos na rede como uma “backdoor”. Os funcionários também podem se desviar dos procedimentos e instalar dispositivos. Um inventário preciso, com rótulos adequados nos dispositivos, permite uma rápida identificação das instalações não aprovadas. Pense em criar uma convenção de nomes oficiais para dispositivos e registre todos os dispositivos com os controles de inventário criados. Rótulos lógicos podem ser empregados com informações, como códigos que podem ser associados ao proprietário, a informações de contato e à sua finalidade.</p>
<p><b>12.3.5</b> Usos aceitáveis da tecnologia</p>	<p><b>12.3.5</b> Verifique se as políticas de utilização definem usos aceitáveis quanto à tecnologia.</p>	<p>Ao definir o uso corporativo aceitável e a localização dos dispositivos e da tecnologia aprovados pela empresa, a empresa fica mais capaz de gerenciar e controlar falhas nas configurações e nos controles operacionais, a fim de garantir que não tenha sido aberta uma “backdoor” para um indivíduo mal-intencionado obter acesso a sistemas críticos e a dados do titular do cartão.</p>
<p><b>12.3.6</b> Locais de rede aceitáveis quanto às tecnologias</p>	<p><b>12.3.6</b> Verifique se as políticas de utilização definem locais de rede aceitáveis quanto à tecnologia.</p>	
<p><b>12.3.7</b> Lista dos produtos aprovados pela empresa</p>	<p><b>12.3.7</b> Verifique se as políticas de utilização incluem uma lista de produtos aprovados pela empresa.</p>	
<p><b>12.3.8</b> Desconexão automática das sessões quanto às tecnologias de acesso remoto após um período específico de inatividade</p>	<p><b>12.3.8</b> Verifique se as políticas de utilização exigem a desconexão automática das sessões quanto às tecnologias de acesso remoto após um período específico de inatividade.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
	<p><b>12.3.8.b</b> Analise as configurações para as tecnologias de acesso remoto para verificar se as sessões de acesso remoto serão desconectadas automaticamente após um período determinado de inatividade.</p>	<p>estiverem em uso (por exemplo, aquelas usadas para dar suporte aos sistemas pelo fornecedor de POS ou por outros fornecedores), o acesso e os riscos à rede são minimizados.</p>
<p><b>12.3.9</b> Ativação de tecnologias de acesso remoto para fornecedores e parceiros de negócio somente quando lhes for necessário, com desativação imediata após o uso</p>	<p><b>12.3.9</b> Verifique se as políticas de utilização exigem a ativação de tecnologias de acesso remoto usadas pelos fornecedores somente quando lhes for necessário, com desativação imediata após o uso.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.3.10</b> Para funcionários que acessam os dados do titular do cartão por meio de tecnologias de acesso remoto, proíba a cópia, a transferência e o armazenamento dos dados do titular do cartão em discos rígidos locais e mídias eletrônicas removíveis, exceto se explicitamente autorizado para uma necessidade comercial definida.</p> <p>Onde houver uma necessidade comercial autorizada, as políticas de utilização devem exigir que os dados sejam protegidos de acordo com todos os requisitos aplicáveis do PCI DSS.</p>	<p><b>12.3.10.a</b> Verifique se as políticas de utilização proíbem a cópia, a transferência ou o armazenamento dos dados do titular do cartão em discos rígidos locais e mídias eletrônicas removíveis ao acessar esses dados por meio de tecnologias de acesso remotas.</p> <p><b>12.3.10.b</b> Para funcionários com autorização adequada, verifique se o uso de políticas exige a proteção dos dados do titular do cartão de acordo com os requisitos do PCI DSS.</p>	<p>Para garantir que os funcionários estejam cientes de suas responsabilidades de não armazenar nem copiar dados do titular do cartão para o computador pessoal local ou outras mídias, sua empresa deve contar com uma política que proíba claramente essas atividades, exceto para os funcionários que foram expressamente autorizados para isso. Armazenar ou copiar dados do titular do cartão em discos rígidos locais ou outras mídias deve estar de acordo com todos os requisitos aplicáveis do PCI DSS.</p>
<p><b>12.4</b> Certifique-se de que a política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança da informação para todos os funcionários.</p>	<p><b>12.4.a</b> Verifique se as políticas de segurança da informação definem claramente as responsabilidades quanto à segurança da informação para todos os funcionários.</p> <p><b>12.4.b</b> Converse com alguns funcionários responsáveis para verificar se eles compreendem as políticas de segurança.</p>	<p>Sem funções e responsabilidades claramente definidas e atribuídas, pode haver uma interação inconsistente com o grupo de segurança, levando a uma implementação não protegida de tecnologias ou ao uso de tecnologias não protegidas ou desatualizadas.</p>
<p><b>12.4.1 Requisito adicional, somente para prestadores de serviços:</b> A gerência executiva deve estabelecer</p>	<p><b>12.4.1.a</b> Analise a documentação para verificar se a gerência executiva atribuiu responsabilidade geral pela manutenção da conformidade do PCI DSS da entidade.</p>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p>responsabilidades pela proteção dos dados de titulares do cartão e um programa de conformidade do PCI DSS, que contemple:</p> <ul style="list-style-type: none"> <li>Responsabilidade geral pela manutenção da conformidade do PCI DSS</li> <li>Definição de diretriz para o programa de conformidade do PCI DSS e comunicação à gerência executiva</li> </ul> <p><b>Observação:</b> Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</p>	<p><b>12.4.1.b</b> Analisar a diretriz corporativa do PCI DSS para verificar se há descrição das condições segundo as quais o programa de conformidade do PCI DSS é organizado e comunicado à gerência executiva.</p>	<p><i>tratar-se de um prestador de serviços.</i></p> <p>A atribuição das responsabilidades referentes à conformidade do PCI DSS pela gerência executiva garante visibilidade do programa de conformidade do PCI DSS e proporciona o surgimento de perguntas adequadas para determinar a eficiência do programa e influenciar as prioridades estratégicas. A responsabilidade geral pelo programa de conformidade do PCI DSS pode ser atribuída a funções individuais e/ou unidades comerciais da organização.</p> <p>A gerência executiva pode incluir posições de nível C, conselho de administração ou equivalente. Os títulos específicos dependerão da estrutura organizacional específica. O nível de detalhes fornecidos à gerência executiva deve ser adequado para a organização e o público-alvo específicos.</p>
<p><b>12.5</b> Atribua a um indivíduo ou a uma equipe as seguintes responsabilidades de gerenciamento da segurança da informação:</p>	<p><b>12.5</b> Analise as políticas e procedimentos de segurança da informação para verificar:</p> <ul style="list-style-type: none"> <li>A atribuição formal da segurança da informação com relação a um Diretor de segurança ou outro membro do gerenciamento que tenha conhecimento sobre segurança.</li> <li>As seguintes responsabilidades da segurança da informação são atribuídas modo formal e específico:</li> </ul>	<p>Cada pessoa ou equipe com responsabilidades pela gestão da segurança da informação deve estar claramente ciente das responsabilidades e das tarefas relacionadas por meio da política específica. Sem essa responsabilidade, falhas nos processos podem dar acesso a recursos críticos ou dados do titular do cartão.</p> <p>As entidades também devem considerar planos de transição e/ou sucessão do pessoal relevante para evitar potenciais lacunas nos procedimentos de segurança, que poderiam resultar em falhas na atribuição de responsabilidades e, portanto, não execução das atribuições.</p>
<p><b>12.5.1</b> Defina, documente e distribua políticas e procedimentos de segurança.</p>	<p><b>12.5.1</b> Verifique se a responsabilidade de definir, documentar e distribuir políticas e procedimentos de segurança está formalmente atribuída.</p>	
<p><b>12.5.2</b> Monitore e analise os alertas e as informações de segurança e distribua para as equipes apropriadas.</p>	<p><b>12.5.2</b> Verifique se a responsabilidade pelo monitoramento e análise dos alertas de segurança e pela distribuição de informações às equipes de gerenciamento adequadas da segurança da informação e das unidades de negócios foi formalmente atribuída.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.5.3</b> Defina, documente e distribua procedimentos de resposta e escalção de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente.</p>	<p><b>12.5.3</b> Verifique se a responsabilidade de definir, documentar e distribuir procedimentos de resposta e escalção de incidentes de segurança é formalmente atribuída.</p>	
<p><b>12.5.4</b> Administre as contas dos usuários, incluindo adições, exclusões e modificações.</p>	<p><b>12.5.4</b> Verifique se a responsabilidade pela administração (adição, exclusão e modificação) das contas dos usuários e do gerenciamento da autenticação é formalmente atribuída.</p>	
<p><b>12.5.5</b> Monitore e controle todos os acessos aos dados.</p>	<p><b>12.5.5</b> Verifique se a responsabilidade por monitorar e controlar todo o acesso aos dados é formalmente atribuída.</p>	
<p><b>12.6</b> Implemente um programa formal sobre conscientização de segurança para conscientizar todos os funcionários em relação à política e aos procedimentos de segurança dos dados do titular do cartão.</p>	<p><b>12.6.a</b> Revise o programa de conscientização de segurança para verificar se ocorre, de fato, a conscientização de todos os funcionários sobre a importância da segurança dos dados do titular do cartão.</p>	<p>Se os usuários não forem treinados sobre as responsabilidades de segurança, as proteções e os processos que forem implementados poderão se tornar ineficazes por causa de erros do funcionário ou ações não intencionais.</p>
	<p><b>12.6.b</b> Analise os procedimentos e a documentação do programa de conscientização de segurança e realize o seguinte:</p>	
<p><b>12.6.1</b> Instrua os funcionários quando da contratação e pelo menos uma vez por ano.</p> <p><b>Observação:</b> Os métodos podem variar dependendo da função de cada funcionário e do nível de acesso aos dados do titular do cartão.</p>	<p><b>12.6.1.a</b> Verifique se o programa de conscientização de segurança fornece vários métodos para transmitir a conscientização e instruir os funcionários (por exemplo, cartazes, cartas, memorandos, treinamento com base na Web, reuniões e promoções).</p>	<p>Se o programa de conscientização de segurança não incluir sessões de atualização anuais, os principais processos e procedimentos de segurança poderão ser esquecidos ou ignorados, resultando em exposição dos recursos críticos e dos dados do titular do cartão.</p>
	<p><b>12.6.1.b</b> Verifique se os funcionários participam do treinamento de conscientização relacionados à contratação pelo menos uma vez por ano.</p>	
	<p><b>12.6.1.c</b> Converse com alguns funcionários para verificar se eles concluíram o treinamento para se conscientizar da importância da segurança dos dados do titular do cartão.</p>	

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.6.2</b> Solicite que os funcionários reconheçam, pelo menos uma vez ao ano, que leram e compreenderam a política e os procedimentos de segurança da empresa.</p>	<p><b>12.6.2</b> Verifique se o programa de conscientização da segurança requer que os funcionários reconheçam, por escrito ou eletronicamente, pelo menos uma vez ao ano, que leram e compreenderam a política de segurança da informação da empresa.</p>	<p>Requerer um reconhecimento dos funcionários, por escrito ou eletronicamente, ajuda a garantir que eles tenham lido e entendido as políticas e os procedimentos de segurança e que eles tenham se comprometido a obedecer a essas políticas.</p>
<p><b>12.7</b> Analise bem os potenciais funcionários antes de contratar a fim de minimizar o risco de invasões a partir de fontes internas. (Exemplos de verificações da formação incluem o histórico do emprego anterior, ficha criminal, histórico de crédito e verificações das referências.)</p> <p><b>Observação:</b> Para os funcionários como caixas de loja, que têm acesso somente a um número do cartão por vez ao viabilizar uma transação, esse requisito é apenas uma recomendação.</p>	<p><b>12.7</b> Converse com a gerência do departamento de Recursos Humanos e verifique se as verificações da formação são realizadas (dentro das restrições das leis locais) antes de contratar funcionários que terão acesso aos dados do titular do cartão ou ao ambiente desses dados.</p>	<p>Executar investigações de histórico completas antes de contratar funcionários que se espera que tenham acesso aos dados do titular do cartão reduz o risco do uso não autorizado de PANs e outros dados do titular do cartão por pessoas com históricos questionáveis ou criminais.</p>
<p><b>12.8</b> Mantenha e implemente políticas e procedimentos para controlar os prestadores de serviços com quem os dados do titular são compartilhados, ou que possam afetar a segurança dos dados, conforme segue:</p>	<p><b>12.8</b> A partir de observações, revisão das políticas e procedimentos e revisão da documentação de apoio, verifique se estão implementados processos para controle dos prestadores de serviços com quem os dados do titular são compartilhados ou que possam afetar a segurança dos dados do titular do cartão, conforme segue:</p>	<p>Se o comerciante ou o prestador de serviço compartilhar os dados do titular do cartão com um prestador de serviço, devem ser aplicados certos requisitos para garantir a proteção contínua desses dados por tais prestadores de serviço.</p> <p>Eis alguns exemplos dos diferentes tipos de prestadores de serviços: áreas de armazenamento de fita de backup, provedores de serviços gerenciados, como empresas de hospedagem na web ou prestadores de serviços de segurança, entidades que recebem dados para fins de determinação de fraude etc.</p>
<p><b>12.8.1</b> Mantenha uma lista dos prestadores de serviços, incluindo uma descrição dos serviços prestados.</p>	<p><b>12.8.1</b> Verifique se há uma lista onde constam os prestadores de serviços e insira uma descrição dos serviços prestados.</p>	<p>Rastrear todos os provedores de serviço identifica quando possíveis riscos se estenderem para fora da organização.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.8.2</b> Mantenha um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do titular do cartão que eles possuem, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente.</p> <p><b>Observação:</b> as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.</p>	<p><b>12.8.2</b> Observe os acordos por escrito e confirme se eles incluem um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do titular do cartão que eles possuem, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente.</p>	<p>O reconhecimento dos prestadores de serviço evidencia o seu compromisso em manter a segurança adequada dos dados do titular do cartão que são obtidos dos clientes. O grau de responsabilidade do prestador de serviços pela segurança dos dados do titular do cartão dependerá do serviço específico e do acordo entre o prestador e a entidade avaliada.</p> <p>Juntamente com o Requisito 12.9, o presente requisito tem por objetivo promover um nível consistente de entendimento entre as partes sobre as responsabilidades aplicáveis ao PCI DSS. Por exemplo, o acordo pode incluir que os requisitos aplicáveis do PCI DSS sejam mantidos como parte do serviço prestado.</p>
<p><b>12.8.3</b> Certifique-se de que haja um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação.</p>	<p><b>12.8.3</b> Verifique se as políticas e procedimentos estão documentados e implementados, incluindo a diligência devida adequada antes da contratação de qualquer prestador de serviços.</p>	<p>O processo garante que qualquer envolvimento de um prestador de serviço seja totalmente vetado internamente pela organização, que deve incluir uma análise de risco antes de estabelecer um relacionamento formal com o prestador de serviços.</p> <p>Os processos de diligência devida e metas específicos variam para cada organização. Exemplos de considerações podem incluir as práticas de relatórios do fornecedor, procedimentos de aviso de violação e resposta a incidentes, detalhes de como as responsabilidades do PCI DSS são atribuídas entre cada parte, como o fornecedor valida sua conformidade com o PCI DSS e qual evidência eles irão fornecer, etc.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.8.4</b> Mantenha um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços.</p>	<p><b>12.8.4</b> Verifique se a entidade mantém um programa para monitorar o status de conformidade com o PCI DSS dos prestadores de serviços pelo menos uma vez ao ano.</p>	<p>Conhecer o status de conformidade do prestador de serviço com o PCI DSS fornece uma garantia a mais de que eles estão de acordo com os mesmos requisitos aos quais a organização está sujeita. Se o provedor oferecer diversos serviços, este requisito se aplicará apenas aos serviços realmente prestados ao cliente e os serviços que estiverem dentro do escopo da avaliação de PCI DSS do cliente.</p>
<p><b>12.8.5</b> Mantenha informações sobre quais requisitos do PCI DSS são administrados por cada prestador de serviços e quais são administrados pela entidade.</p>	<p><b>12.8.5</b> Verifique se a entidade mantém informações sobre quais requisitos do PCI DSS são administrados por cada prestador de serviços e quais são administrados pela entidade.</p>	<p>A informação específica que uma entidade mantém dependerá do acordo particular com seus fornecedores, o tipo de serviço, etc. O objetivo é que a entidade avaliada entenda quais requisitos do PCI DSS seus fornecedores concordaram em atender.</p>
<p><b>12.9 Requisito adicional, somente para prestadores de serviços:</b> Os prestadores de serviços reconhecem por escrito aos clientes que eles são responsáveis pela segurança dos dados do titular do cartão que eles possuem, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente.</p> <p><b>Observação:</b> as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.</p>	<p><b>12.9 Procedimento de teste adicional somente para avaliação de prestadores de serviços:</b> Revise as políticas e os procedimentos do prestador de serviços e observe os modelos dos acordos escritos para confirmar se o prestador reconhece por escrito aos clientes que manterá todos os requisitos aplicáveis do PCI DSS segundo o limite em que acessa ou, de outra forma, armazena, processa ou transmite dados do titular do cartão em nome do cliente, ou segundo o limite em que poderia impactar a segurança do ambiente de dados do titular do cartão do cliente.</p>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>Juntamente com o Requisito 12.8.2, o presente requisito tem por objetivo promover um nível consistente de entendimento entre os prestadores de serviços e seus clientes sobre as responsabilidades aplicáveis ao PCI DSS. O reconhecimento dos prestadores de serviço evidencia o seu compromisso em manter a segurança adequada dos dados do titular do cartão que são obtidos dos clientes.</p> <p>Políticas e procedimentos internos do prestador de serviços relacionados ao processo de engajamento do cliente e aos modelos usados para acordos por escrito devem incluir a provisão do reconhecimento aplicável do cliente referente ao PCI DSS. O método pelo qual o prestador de serviços fornece o reconhecimento por escrito deve ser acordado entre o fornecedor e seus clientes.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.10</b> Implemente um plano de resposta a incidentes. Prepare-se para reagir imediatamente a uma falha no sistema.</p>	<p><b>12.10</b> Analise o plano de resposta a incidentes e os procedimentos relatados para verificar se a entidade está preparada para reagir imediatamente a uma violação no sistema realizando o que segue:</p>	<p>Sem um plano de resposta a incidentes de segurança completo que seja adequadamente disseminado, lido e entendido pelas partes responsáveis, a confusão e a falta de uma resposta unificada podem criar mais tempo ocioso para a empresa, exposição pública desnecessária e novas responsabilidades legais.</p>
<p><b>12.10.1</b> Crie o plano de resposta a incidentes para ser implementado no caso de violações do sistema. Certifique-se de que o plano aborda o seguinte, pelo menos:</p> <ul style="list-style-type: none"> <li>• Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo a notificação às bandeiras de pagamento, pelo menos</li> <li>• Procedimentos de resposta específicos a incidentes</li> <li>• Procedimentos de recuperação e continuidade dos negócios</li> <li>• Processos de backup dos dados</li> <li>• Análise dos requisitos legais visando ao relato dos comprometimentos</li> <li>• Abrangência e resposta de todos os componentes críticos do sistema</li> <li>• Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras.</li> </ul>	<p><b>12.10.1.a</b> Verifique se o plano de resposta a incidentes inclui:</p> <ul style="list-style-type: none"> <li>• Funções, responsabilidades e estratégias de comunicação no caso de um comprometimento, incluindo a notificação às bandeiras de pagamento, pelo menos</li> <li>• Procedimentos de resposta específicos a incidentes</li> <li>• Procedimentos de recuperação e continuidade dos negócios</li> <li>• Processos de backup dos dados</li> <li>• Análise dos requisitos legais referentes ao relato dos comprometimentos (por exemplo, Lei 1386 da Califórnia, que exige a notificação dos clientes afetados no caso de um comprometimento real ou suspeito para qualquer negócio que seja realizado com moradores da Califórnia em seu banco de dados)</li> <li>• Abrangência e resposta de todos os componentes críticos do sistema</li> <li>• Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras.</li> </ul> <p><b>12.10.1.b</b> Converse com os funcionários e revise a documentação a partir de incidentes ou alertas relatados previamente para verificar se o plano e os procedimentos de resposta ao incidente documentado foram seguidos.</p>	<p>O plano de resposta a incidentes deve ser completo e conter todos os elementos-chave para permitir que sua empresa reaja com eficiência no caso de uma violação que possa causar impacto nos dados do titular do cartão.</p>
<p><b>12.10.2</b> Revise e teste o plano, inclusive todos os elementos previstos no Requisito 12.10.1, pelo menos, anualmente.</p>	<p><b>12.10.2</b> Converse com o pessoal e revise a documentação de teste para verificar se o plano é testado, pelo menos, anualmente, e se o teste considera todos os elementos enumerados no Requisito 12.10.1.</p>	<p>Sem testes adequados, etapas essenciais podem ser perdidas, o que poderia aumentar a exposição durante um incidente.</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<p><b>12.10.3</b> Designe equipes específicas para estarem disponíveis em tempo integral para responder aos alertas.</p>	<p><b>12.10.3</b> Verifique, por meio da observação, análise das políticas e entrevistas com funcionários responsáveis se a equipe designada está disponível para cobertura de monitoramento e resposta a incidentes em tempo integral para qualquer evidência de atividade não autorizada, detecção de pontos de acesso sem fio não autorizados, alertas de IDS críticos e/ou relatórios de sistemas críticos não autorizados ou alterações nos arquivos de conteúdo.</p>	<p>Sem uma equipe de reação a incidentes treinada e prontamente disponível, podem ocorrer danos extensos à rede e dados e sistemas críticos podem ficar “poluídos” pelo manuseio inadequado dos sistemas almejados. Isso pode evitar o sucesso de uma investigação pós-incidente.</p>
<p><b>12.10.4</b> Forneça treinamento adequado à equipe que é responsável pela resposta às falhas do sistema.</p>	<p><b>12.10.4</b> Verifique, por meio de observação, análises das políticas e entrevistas com os funcionários responsáveis se a equipe com responsabilidades de resposta a violações de segurança são treinadas periodicamente.</p>	
<p><b>12.10.5</b> Inclua alertas a partir dos sistemas de monitoramento de segurança, incluindo, entre outros, detecção e prevenção contra invasões, firewalls e sistemas de monitoramento da integridade dos arquivos.</p>	<p><b>12.10.5</b> Verifique, por meio da observação e da análise dos processos, se o monitoramento e a resposta aos alertas a partir dos sistemas de monitoramento da segurança são abordados no plano de resposta a incidentes.</p>	<p>Esses sistemas de monitoramento são feitos para se concentrar em possíveis riscos aos dados, são essenciais para se tomar uma ação rápida para evitar uma violação e devem estar incluídos nos processos de resposta a incidentes.</p>
<p><b>12.10.6</b> Desenvolva um processo para modificar e aprimorar o plano de resposta a incidentes, de acordo com as lições aprendidas e para incorporar os desenvolvimentos do setor.</p>	<p><b>12.10.6</b> Verifique, por meio da observação, da análise das políticas e entrevistas com os funcionários responsáveis se há um processo para modificar e aprimorar o plano de resposta a incidentes, de acordo com as lições aprendidas e para incorporar os desenvolvimentos do setor.</p>	<p>Incorporar as “lições aprendidas” no plano de reação a incidentes depois de um incidente ajuda a manter o plano atualizado e capaz de reagir às ameaças que surgirem e às tendências de segurança.</p>
<p><b>12.11 Requisito adicional, somente para prestadores de serviços:</b> Proceda à análise, pelo menos, trimestralmente para confirmar se os funcionários estão cumprindo as políticas de segurança e os procedimentos operacionais. As análises devem abranger os seguintes processos:</p> <ul style="list-style-type: none"> <li>• Revisão diária dos registros</li> <li>• Comentários de conjunto de regras de firewall</li> <li>• Aplicação de padrões de configuração em novos sistemas</li> </ul>	<p><b>12.11.a</b> Analise as políticas e os procedimentos para verificar se há processos definidos para revisão e confirmação de que a equipe está cumprindo os procedimentos operacionais e as políticas de segurança; a análise deve abranger:</p> <ul style="list-style-type: none"> <li>• Revisão diária dos registros</li> <li>• Comentários de conjunto de regras de firewall</li> <li>• Aplicação de padrões de configuração em novos sistemas</li> <li>• Responder a alertas de segurança</li> <li>• Alterar processos de gestão</li> </ul>	<p><b>Observação:</b> Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</p> <p>A confirmação regular do cumprimento das políticas e dos procedimentos de segurança garante que os controles previstos encontram-se ativos e em funcionamento conforme pretendido. O objetivo das análises não é executar outras exigências do PCI DSS novamente, porém confirmar se os procedimentos estão sendo cumpridos</p>

Requisitos do PCI DSS	Procedimentos de teste	Orientação
<ul style="list-style-type: none"> <li>• Responder a alertas de segurança</li> <li>• Alterar processos de gestão</li> </ul> <p><i>Observação: Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i></p>	<p><b>12.11.b</b> Converse com o pessoal responsável e examine os registros das análises para verificar se as análises ocorrem, pelo menos, trimestralmente.</p>	<p>conforme o esperado.</p>
<p><b>12.11.1 Requisito adicional, somente para prestadores de serviços:</b> Mantenha a documentação do processo de revisão trimestral e considere:</p> <ul style="list-style-type: none"> <li>• Documentar os resultados das revisões</li> <li>• Revisar e assinar os resultados por funcionários com atribuição de responsabilidade no programa de conformidade do PCI DSS</li> </ul> <p><i>Observação: Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i></p>	<p><b>12.11.1</b> Examinar a documentação das revisões trimestrais para verificar se incluem:</p> <ul style="list-style-type: none"> <li>• Documentar os resultados das revisões</li> <li>• Revisar e assinar os resultados por funcionários com atribuição de responsabilidade no programa de conformidade do PCI DSS</li> </ul>	<p><i>Observação: Este requisito aplica-se somente quando a entidade que está sendo avaliada tratar-se de um prestador de serviços.</i></p> <p>A intenção das verificações independentes é confirmar se as atividades de segurança estão sendo executadas regularmente. As revisões também podem ser usadas para verificar se a evidência adequada está sendo mantida (por exemplo, logs de auditoria, relatórios de varredura de vulnerabilidade, revisões do firewall etc.), a fim de auxiliar na preparação da entidade para a próxima avaliação do PCI DSS.</p>

## Apêndice A: Requisitos adicionais do PCI DSS

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

- Apêndice A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada
- Apêndice A2: Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS
- Apêndice A3: Validação Suplementar de Entidades Designadas

Informações sobre orientação e aplicabilidade são fornecidas a cada seção.

## Apêndice A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada

Conforme mencionado nos Requisitos 12.8 e 12.9, todos os provedores de serviços com acesso aos dados do titular do cartão (inclusive, provedores de hospedagem compartilhada) devem aderir ao PCI DSS. Além disso, o Requisito 2.6 afirma que os provedores de hospedagem compartilhada devem proteger o ambiente hospedado e os dados de cada entidade. Portanto, os provedores de hospedagem compartilhada também devem estar em conformidade com os requisitos nesse Apêndice.

A1 Requisitos	Procedimentos de teste	Orientação
<p><b>A1</b> Proteja os dados e o ambiente hospedado de cada entidade (ou seja, do comerciante, prestador de serviços ou outra entidade), de acordo com os itens A1.1 a A1.4:</p> <p>O provedor de hospedagem deve cumprir esses requisitos e todas as outras seções relevantes do PCI DSS.</p> <p><b>Observação:</b> Mesmo que o provedor de hospedagem cumpra esses requisitos, a conformidade da entidade que usa o provedor de hospedagem não está assegurada. Cada entidade deve estar em conformidade com o PCI DSS e validar a conformidade, conforme aplicável.</p>	<p><b>A1</b> Especificamente para uma avaliação do PCI DSS de um provedor de hospedagem compartilhada, para verificar se os provedores de hospedagem compartilhada protegem o ambiente hospedado e os dados das entidades (comerciantes e prestadores de serviços), selecione um exemplo de servidores (Microsoft Windows e Unix/Linux) dentre vários exemplos representativos de comerciantes e prestadores de serviços, e execute o que está descrito nos itens A1.1 a A1.4 abaixo:</p>	<p>O Apêndice A do PCI DSS é destinado a provedores de hospedagem compartilhada que desejam fornecer aos clientes do comerciante e/ou prestador de serviço um ambiente de hospedagem em conformidade com o PCI DSS.</p>
<p><b>A.1.1</b> Certifique-se de que cada entidade execute somente os processos com acesso ao ambiente de dados do titular do cartão daquela entidade.</p>	<p><b>A.1.1</b> Se um provedor de hospedagem compartilhada permitir que as entidades (por exemplo, comerciantes ou prestadores de serviços) executem seus próprios aplicativos, verifique se os processos dos aplicativos são executados mediante identificação exclusiva da entidade. Por exemplo:</p> <ul style="list-style-type: none"> <li>• Nenhuma entidade no sistema pode usar um ID de usuário do servidor Web compartilhado.</li> <li>• Todos os scripts CGI usados por uma entidade devem ser criados e executados como o ID do usuário exclusivo da entidade.</li> </ul>	<p>Se um comerciante ou prestador de serviço puder executar seus próprios aplicativos no servidor compartilhado, eles devem ser executados com o ID de usuário do comerciante ou prestador de serviço e não como um usuário privilegiado.</p>

A1 Requisitos	Procedimentos de teste	Orientação
<p><b>A.1.2</b> Restrinja o acesso e os privilégios de cada entidade somente ao próprio ambiente de dados do titular do cartão.</p>	<p><b>A.1.2.a</b> Verifique se a ID do usuário de qualquer processo de aplicativo não concede privilégios (raiz/admin).</p> <p><b>A.1.2.b</b> Verifique se cada entidade (comerciante, prestador de serviços) leu, registrou ou executou permissões exclusivamente referentes aos arquivos e diretórios que possui ou para os arquivos de sistema necessários (restritos por meio das permissões do sistema de arquivo, listas de controle de acesso, chroot, jailshell etc.).</p> <p><b>Importante:</b> Os arquivos de uma entidade não podem ser compartilhados em grupo.</p> <p><b>A.1.2.c</b> Verifique se os usuários da entidade não têm acesso de escrita aos binários compartilhados do sistema.</p> <p><b>A.1.2.d</b> Verifique se a visualização das entradas de registro é restrita à entidade detentora.</p> <p><b>A.1.2.e</b> Para garantir que as entidades não possam monopolizar os recursos do servidor para explorar vulnerabilidades (por exemplo, condições de erro, aceleração e reinicialização, resultando, por exemplo, em sobrecargas de buffer), verifique se as restrições foram implementadas para a utilização destes recursos do sistema:</p> <ul style="list-style-type: none"> <li>• Espaço em disco</li> <li>• Largura de banda</li> <li>• Memória</li> <li>• CPU</li> </ul>	<p>Para garantir que os acessos e os privilégios estejam restritos, de forma que cada comerciante ou prestador de serviço só tenha acesso ao próprio ambiente dos dados, considere o seguinte:</p> <ol style="list-style-type: none"> <li>1. Privilégios do ID do usuário do servidor Web do prestador de serviços ou do comerciante;</li> <li>2. Permissões concedidas para ler, escrever e executar arquivos;</li> <li>3. Permissões concedidas para escrever em binários do sistema;</li> <li>4. Permissões concedidas para arquivos de log dos comerciantes e prestadores de serviços; e</li> <li>5. Controles para garantir que um comerciante ou prestador de serviços não possa monopolizar recursos do sistema.</li> </ol>
<p><b>A1.3</b> Certifique-se de que os registros e percursos de auditoria estão ativados e são exclusivos para o ambiente de dados do titular do cartão de cada entidade, além de estarem em conformidade com o Requisito 10 do PCI DSS.</p>	<p><b>A1.3</b> Verifique se o provedor de hospedagem compartilhada ativou os registros conforme segue, para o ambiente de cada comerciante e prestador de serviços:</p> <ul style="list-style-type: none"> <li>• Os registros são ativados para os aplicativos de terceiros comuns.</li> <li>• Como padrão, os registros estão ativados.</li> <li>• Os registros estão disponíveis para análise pela entidade detentora.</li> <li>• As localizações dos registros são informadas com clareza à entidade detentora.</li> </ul>	<p>Os registros devem estar disponíveis em um ambiente de hospedagem compartilhado, de forma que os comerciantes e prestadores de serviço tenham acesso e consigam analisar os logs específicos ao ambiente dos dados do titular do cartão.</p>

A1 Requisitos	Procedimentos de teste	Orientação
<p><b>A1.4</b> Permita que os processos providenciem investigação forense oportuna em caso de comprometimento a qualquer comerciante ou prestador de serviços hospedado.</p>	<p><b>A1.4</b> Verifique se o provedor de hospedagem compartilhada definiu políticas que proporcionem uma investigação forense oportuna dos servidores relacionados no caso de comprometimento.</p>	<p>Os provedores de hospedagem compartilhada devem ter processos para fornecer uma resposta rápida e fácil no caso de uma investigação forense ser necessária para um comprometimento, até o nível adequado de detalhes, de forma que os detalhes individuais do comerciante ou do prestador de serviço estejam disponíveis.</p>

## Apêndice A2: Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS

Entidades que usam SSL e TLS antigo devem trabalhar pelo upgrade para obtenção de um protocolo criptográfico robusto, assim que possível. Além disso, SSL e/ou TLS antigo não devem ser introduzidos em ambientes onde os protocolos mencionados já não existem mais. No momento da publicação, as vulnerabilidades conhecidas são difíceis de explorar em ambientes de pagamento POS POI. No entanto, novas vulnerabilidades poderiam surgir a qualquer momento, e cabe à organização manter-se atualizada em relação às tendências em vulnerabilidade e determinar se estão ou não suscetíveis a formas de ataque conhecidas.

Os requisitos do PCI DSS diretamente afetados são:

- Requisito 2.2.3** Implementar recursos de segurança adicionais para todos os serviços, protocolos ou daemons exigidos considerados não seguros.
- Requisito 2.3** Criptografar todo acesso administrativo que não utiliza console com criptografia robusta.
- Requisito 4.1** Usar protocolos de segurança e criptografia robusta para proteger dados sensíveis do titular do cartão durante a transmissão em redes abertas e públicas.

Os protocolos SSL e TLS antigo não devem ser usados como controle de segurança para atender aos presentes requisitos. Para oferecer suporte a entidades trabalhando para migrar do SSL/TSL antigo, as disposições seguintes são incluídas:

- Novas implementações não devem usar SSL ou TLS antigo como controle de segurança.
- Até 30 de junho de **2016**, todos os prestadores de serviço deverão oferecer serviço seguro.
- Após 30 de junho de **2018**, todas as entidades deverão interromper o uso do SSL/TSL antigo como controle de segurança e usar somente versões seguras do protocolo (a concessão para determinados terminais POS POI é descrita no último item abaixo).
- Antes de 30 de junho de 2018, implementações existentes que usam SSL ou TLS antigo devem estabelecer um plano formal de migração e redução de riscos.
- Terminais POS POI (e pontos de terminação SSL/TLS aos quais se conectam) que podem ser verificados e considerados não suscetíveis a ataques conhecidos via SSL e TLS antigo, podem continuar a usá-los como controle de segurança após 30 de junho de 2018.

Este Apêndice aplica-se a entidades que usam SSL/TLS antigo como controle de segurança para proteger o CDE e/ou CHD (por exemplo, SSL/TLS antigo usado para atender aos requisitos 2.2.3, 2.3 ou 4.1 do PCI DSS). Consulte as *Informações Suplementares atualizadas do PCI SSC referentes à Migração do SSL/TLS antigo*, para obter mais orientações sobre o uso dos protocolos SSL/TSL antigo.

A2 Requisitos	Procedimentos de teste	Orientação
<p><b>A2.1</b> Nos locais onde terminais POS POI (e pontos de terminação SSL/TLS aos quais se conectam) usam SSL e/ou TLS antigo, a entidade deve:</p> <ul style="list-style-type: none"> <li>• Confirmar se os dispositivos não estão suscetíveis a ataques conhecidos para os citados protocolos.</li> </ul> <p><b>Ou:</b></p> <ul style="list-style-type: none"> <li>• Implementar um plano de migração e mitigação de risco.</li> </ul>	<p><b>A2.1</b> Para terminais POS POI (e pontos de terminação SSL/TLS aos quais se conectam) usando SSL e/ou TLS antigo:</p> <ul style="list-style-type: none"> <li>• Confirme se a entidade apresenta documentação (por exemplo, documentação do fornecedor, detalhes de configuração do sistema/rede etc.) que verifica se os dispositivos não estão suscetíveis a ataques conhecidos para os protocolos SSL/TLS antigo.</li> </ul> <p>Ou:</p> <ul style="list-style-type: none"> <li>• Concluir A2.2 abaixo.</li> </ul>	<p>POIs podem continuar a usar os protocolos SSL/TLS antigo quando houver comprovação de que o POI não está suscetível a ataques atualmente conhecidos. No entanto, o protocolo SSL é uma tecnologia ultrapassada possivelmente sujeita a novas vulnerabilidades de segurança no futuro; portanto, é altamente recomendável que ambientes POI procedam ao upgrade para um protocolo seguro, assim que possível. Se não houver necessidade dos protocolos SSL/TLS antigo no ambiente, o uso e plano alternativo para estas versões devem ser desativados.</p> <p>Se o ambiente POS POI estiver suscetível a ataques conhecidos, o planejamento de migração para uma alternativa segura deve ser iniciado imediatamente.</p> <p><b>Observação:</b> A concessão para POS POIs que não estão suscetíveis a ataques é baseada nos riscos atuais e conhecidos. Se novos ataques forem introduzidos, em relação aos quais os ambientes POI sejam suscetíveis, os ambientes POI deverão ser atualizados.</p>

A2 Requisitos	Procedimentos de teste	Orientação
<p><b>A2.2</b> Entidades com implementações vigentes (outras que não conforme previstas na seção A2.1), que usam os protocolos SSL e/ou TLS antigo devem estabelecer um plano formal de migração e redução de riscos.</p>	<p><b>A2.2</b> Rever o plano de migração e redução de riscos documentado, para verificar se inclui:</p> <ul style="list-style-type: none"> <li>• Descrição do uso, incluindo dados que estão sendo transmitidos, tipos e número de sistemas que usam e/ou oferecem suporte para os protocolos SSL/TLS antigo, tipo de ambiente;</li> <li>• Resultados da avaliação de risco e implementação de controles para redução de risco;</li> <li>• Descrição dos processos para monitorar as novas vulnerabilidades associadas com SSL/TLS antigo;</li> <li>• Descrição de processos de controle de alterações que são implementados para garantir que o SSL/TLS antigo não seja implementado em novos ambientes;</li> <li>• Visão geral do plano do projeto de migração, com data prevista para conclusão da migração até, no máximo, 30 de junho de 2018.</li> </ul>	<p>O plano de migração e redução de risco é um documento elaborado pela entidade detalhando seus planos de migração para um protocolo seguro, além de descrever os controles usados pela entidade para reduzir o risco associado aos protocolos SSL/TSL antigo até que a migração seja concluída.</p> <p>Consulte as Informações Suplementares atualizadas do PCI SSC referentes à Migração do SSL/TLS antigo, para obter orientações adicionais sobre redução de riscos e planos de migração.</p>
<p><b>A2.3 Requisito adicional, somente para prestadores de serviços:</b> Até 30 de junho de 2016, todos os prestadores de serviço deverão oferecer serviço seguro.</p> <p><b>Observação:</b> Antes de 30 de junho de 2016, o prestador de serviços deve ter uma opção de protocolo seguro incluída na sua oferta de serviços, <b>ou</b> ter um plano de redução de riscos e migração documentado (conforme A2.2) que inclui uma meta de data para a oferta de uma opção de protocolo seguro antes de 30 de junho de 2016. Após esta data, todos os provedores de serviço devem oferecer uma opção de protocolo seguro para o seu serviço.</p>	<p><b>A2.3</b> Analise as configurações do sistema e a documentação de apoio para verificar se o prestador de serviços oferece uma opção de protocolo seguro para o serviço.</p>	<p>Consulte o termo "Prestadores de serviços" no Glossário de termos, abreviaturas e acrônimos do <i>PCI DSS</i> e do <i>PA-DSS</i> para mais esclarecimentos.</p>

### **Apêndice A3: Validação Suplementar de Entidades Designadas (DESV)**

Este apêndice se aplica apenas a entidades designadas por uma empresa de pagamento ou adquirente que exigem uma validação adicional dos requisitos existentes do PCI DSS. São exemplos de entidades às quais este Apêndice **poderia** se aplicar:

- Entidades que armazenam, processam e/ou transmitem grandes volumes de dados de titulares de cartão,
- Entidades que fornecem pontos de agregação para dados de titulares de cartão, ou
- Entidades vítimas de violações consecutivas ou significativas aos dados de titulares de cartão.

As etapas de validação suplementar destinam-se a aumentar a garantia de que os controles do PCI DSS serão efetiva e continuamente mantidos, por meio da validação de processos de rotina (BAU), incremento da validação e considerações do escopo.

As etapas adicionais de validação constantes neste documento estão organizadas de acordo com as áreas de controle seguintes:

**A3.1** *Implementar um programa de conformidade do PCI DSS.*

**A3.2** *Documentar e validar o escopo do PCI DSS.*

**A3.3** *PCI DSS validado e incorporado às atividades de rotina (BAU).*

**A3.4** *Controlar e gerenciar o acesso lógico ao ambiente de dados do titular do cartão.*

**A3.5** *Identificar e solucionar eventos suspeitos.*

**Observação:** *Alguns requisitos estabelecem prazos definidos (por exemplo, no mínimo, trimestral ou semestralmente), segundo os quais determinadas atividades devem ser executadas. Para a avaliação inicial deste documento, não é necessário que as atividades tenham sido realizadas segundo cada período de tempo no ano anterior, se o avaliador verificar que:*

- 1) *A atividade foi realizada de acordo com a exigência aplicável, no prazo mais recente (ou seja, o trimestre ou semestre mais recente), e*
- 2) *A entidade registrou as políticas e os procedimentos para continuar exercendo a atividade segundo o prazo definido.*

*Para os anos subsequentes após a avaliação inicial, as atividades devem ter sido realizadas segundo cada período de tempo estabelecido (por exemplo, atividades trimestrais devem ter sido realizadas para cada um dos quatro trimestres do ano anterior).*

**Observação:** *A entidade deve ser submetida a uma avaliação conforme este Apêndice **SOMENTE se instruída a fazê-lo** por um adquirente ou marca do sistema de pagamento.*

A3 Requisitos	Procedimentos de teste	Orientação
<b>A3.1 Implementar um programa de conformidade do PCI DSS</b>		
<p><b>A3.1.1</b> A gerência executiva deve estabelecer responsabilidades pela proteção dos dados de titulares do cartão e um programa de conformidade do PCI DSS, que contemple:</p> <ul style="list-style-type: none"> <li>• Responsabilidade geral pela manutenção da conformidade do PCI DSS</li> <li>• Definição de diretriz para o programa de conformidade do PCI DSS</li> <li>• Comunicar atualizações à gerência executiva e ao conselho de administração sobre as iniciativas e problemas de conformidade em relação ao PCI DSS, inclusive atividades de correção, pelo menos, anualmente</li> </ul> <p><b>Referência do PCI DSS:</b> Requisito 12</p>	<p><b>A3.1.1.a</b> Analise a documentação para verificar se a gerência executiva atribuiu responsabilidade geral pela manutenção da conformidade do PCI DSS da entidade.</p> <p><b>A3.1.1.b</b> Analisar a diretriz corporativa do PCI DSS para verificar se há descrição das condições segundo as quais o programa de conformidade do PCI DSS é organizado.</p> <p><b>A3.1.1.c</b> Analisar as apresentações e/ou minutas das reuniões da gerência executiva e do conselho administrativo para garantir que as iniciativas e atividades de correção relacionadas à conformidade do PCI DSS sejam comunicadas, pelo menos, anualmente.</p>	<p>A atribuição das responsabilidades referentes à conformidade do PCI DSS pela gerência executiva garante visibilidade do programa de conformidade do PCI DSS e proporciona o surgimento de perguntas adequadas para determinar a eficiência do programa e influenciar as prioridades estratégicas. A responsabilidade geral pelo programa de conformidade do PCI DSS pode ser atribuída a funções individuais e/ou unidades comerciais da organização.</p>
<p><b>A3.1.2</b> Um programa formal de conformidade do PCI DSS deve ser estabelecido e incluir:</p> <ul style="list-style-type: none"> <li>• Definição das atividades para manutenção e monitoramento geral relacionado à conformidade do PCI DSS, inclusive atividades de rotina</li> <li>• Processos de avaliação anual do PCI DSS</li> <li>• Processos de validação contínua dos requisitos do PCI DSS (por exemplo: diariamente, semanalmente, trimestralmente etc., conforme o caso, por requisito)</li> <li>• Processo para realização de análise de impacto comercial para determinar os</li> </ul>	<p><b>A3.1.2.a</b> Analise as políticas e os procedimentos de segurança das informações para verificar se os processos estão definidos para o que segue:</p> <ul style="list-style-type: none"> <li>• Manutenção e monitoramento geral relacionado à conformidade do PCI DSS, inclusive atividades comerciais de rotina</li> <li>• Avaliação anual/avaliações anuais do PCI DSS</li> <li>• Validação contínua dos requisitos do PCI DSS</li> <li>• Análise de impacto comercial para determinar os impactos potenciais do PCI DSS sobre decisões estratégicas comerciais</li> </ul>	<p>Um programa formal de conformidade permite que a organização monitore a saúde dos controles de segurança, seja proativa em caso de falha no controle e comunicar com eficiência as atividades e o status de conformidade em toda a organização.</p> <p>O programa de conformidade do PCI DSS pode ser dedicado ou parte de um programa principal de conformidade e/ou governança, e deve apresentar uma metodologia bem definida capaz de demonstrar uma avaliação coerente e eficaz. Exemplo de metodologias: Círculo - ciclo - roda de Deming (Deming Circle of Plan-Do-Check-Act, PDCA), ISO 27001, COBIT, DMAIC e Six Sigma.</p> <p style="text-align: right;"><i>(Continua na próxima página)</i></p>

A3 Requisitos	Procedimentos de teste	Orientação
<p>impactos potenciais do PCI DSS sobre decisões estratégicas comerciais</p> <p><b>Referência do PCI DSS:</b> Requisitos 1-12</p>		
	<p><b>A3.1.2.b</b> Converse com o pessoal e observe as atividades de conformidade para verificar se os processos definidos são implementados conforme a seguir:</p> <ul style="list-style-type: none"> <li>• Manutenção e monitoramento geral relacionado à conformidade do PCI DSS, inclusive atividades comerciais de rotina</li> <li>• Avaliação anual/avaliações anuais do PCI DSS</li> <li>• Validação contínua dos requisitos do PCI DSS</li> <li>• Análise de impacto comercial para determinar os impactos potenciais do PCI DSS sobre decisões estratégicas comerciais</li> </ul>	<p>A manutenção e o monitoramento da conformidade geral do PCI DSS na organização incluem a identificação das atividades a serem executadas diária, semanal, mensal, trimestral ou anualmente, e a garantia de que as atividades são realizadas em plena conformidade (por exemplo, com o uso de autoavaliação de segurança ou metodologia PDCA).</p> <p>Exemplos de decisões estratégicas comerciais que devem ser analisadas em relação aos impactos potenciais do PCI DSS podem incluir fusões e aquisições, aquisição de novas tecnologias ou novos canais de aceitação de pagamento.</p>
<p><b>A3.1.3</b> Funções e responsabilidades referentes à conformidade do PCI DSS devem ser especificamente definidas e formalmente atribuídas a uma ou mais equipes, considerando, pelo menos, as seguintes:</p> <ul style="list-style-type: none"> <li>• Gerenciamento das atividades comerciais de rotina do PCI DSS</li> <li>• Gerenciamento das avaliações anuais do PCI DSS</li> <li>• Gerenciamento da validação contínua dos requisitos do PCI DSS (por exemplo: diariamente, semanalmente, trimestralmente etc., conforme o caso, por requisito)</li> <li>• Gerenciamento da análise de impacto</li> </ul>	<p><b>A3.1.3.a</b> Analise os procedimentos e as políticas de segurança da informação e converse com o pessoal para verificar se as funções e responsabilidades estão claramente definidas e se as obrigações atribuídas consideram, pelo menos, o seguinte:</p> <ul style="list-style-type: none"> <li>• Gerenciamento das atividades comerciais de rotina do PCI DSS</li> <li>• Gerenciamento das avaliações anuais do PCI DSS</li> <li>• Gerenciamento da validação contínua dos requisitos do PCI DSS (por exemplo: diariamente, semanalmente, trimestralmente etc., conforme o caso, por requisito)</li> <li>• Gerenciamento da análise de impacto comercial para determinar os impactos potenciais do PCI DSS sobre decisões estratégicas comerciais</li> </ul>	<p>A definição formal das funções e responsabilidades específicas referentes à conformidade do PCI DSS contribui para garantir a responsabilidade e o monitoramento dos esforços contínuos de conformidade do PCI DSS. As funções podem ser atribuídas a um único responsável ou a diversos responsáveis, em diferentes aspectos. A responsabilidade deve ser atribuída a indivíduos com autoridade para tomar decisões arriscadas e sobre quem recai a responsabilidade pela função específica. As obrigações devem ser formalmente definidas e os responsáveis devem ser capazes de demonstrar compreensão acerca das responsabilidades assumidas.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p>comercial para determinar os impactos potenciais do PCI DSS sobre decisões estratégicas comerciais</p> <p><b>Referência do PCI DSS:</b> Requisito 12</p>	<p><b>A3.1.3.b</b> Converse com o pessoal responsável, verifique se estão familiarizados e se executam as responsabilidades atribuídas referentes à conformidade do PCI DSS.</p>	
<p><b>A3.1.4</b> Ofereça treinamento em segurança da informação e/ou atualização do PCI DSS, pelo menos, anualmente, para o pessoal com responsabilidade de conformidade relacionada ao PCI DSS (conforme identificação em A3.1.3).</p> <p><b>Referência do PCI DSS:</b> Requisito 12</p>	<p><b>A3.1.4.a</b> Analise as políticas e os procedimentos de segurança da informação para verificar se o treinamento em segurança da informação e/ou PCI DSS é exigido, pelo menos, anualmente, para cada função com responsabilidades de conformidade relacionadas ao PCI DSS.</p> <p><b>A3.1.4.b</b> Converse com o pessoal e analise os certificados de participação ou outros registros, para verificar se a equipe com responsabilidades de conformidade relacionadas ao PCI DSS receberam treinamento em segurança da informação e/ou atualização do PCI DSS, pelo menos, anualmente.</p>	<p>O pessoal responsável pela conformidade do PCI DSS tem necessidades de formação específicas superiores às normalmente fornecidas pelo treinamento geral em conscientização da segurança. Indivíduos com responsabilidades de conformidade relacionadas ao PCI DSS devem receber treinamento especializado que, além da sensibilização geral frente à segurança das informações, aborde tópicos, habilidades, processos ou metodologias de segurança específicos que devem ser obedecidos para que desempenhem com eficácia as responsabilidades de conformidade que lhe foram atribuídas.</p> <p>O treinamento pode ser oferecido por terceiros — por exemplo, SANS ou PCI SSC (conscientização relacionada ao PCI, PCIP e ISA), marcas de pagamento e adquirentes — ou treinamento interno. O conteúdo do treinamento deve aplicar-se à função específica e estar atualizado, considerando as mais recentes ameaças à segurança e/ou versão do PCI DSS.</p> <p>Para obter orientação adicional sobre o desenvolvimento de conteúdo de treinamento em segurança adequado para funções especializadas, consulte as Informações Suplementares do PCI SSC sobre <i>Práticas recomendadas para a implementação de um programa de conscientização em segurança</i>.</p>

**A3.2 Documentar e validar o escopo do PCI DSS**

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.1</b> Registre e confirme a precisão do escopo do PCI DSS, pelo menos, trimestralmente e após alterações significativas ao ambiente no escopo. A validação trimestral do escopo validação deve incluir, no mínimo:</p> <ul style="list-style-type: none"> <li>• Identificação de todas as redes no escopo e componentes do sistema</li> <li>• Identificação de todas as redes fora do escopo e justificativa para tanto, incluindo descrições de todos os controles de segmentação implementados</li> <li>• Identificação de todas as entidades conectadas —p. ex., entidades de terceiros com acesso ao ambiente de dados do titular do cartão (CDE)</li> </ul> <p><b>Referência do PCI DSS:</b> <i>Escopo dos requisitos do PCI DSS</i></p>	<p><b>A3.2.1.a</b> Analise os resultados documentados das revisões do escopo e converse com o pessoal para verificar se as revisões ocorrem:</p> <ul style="list-style-type: none"> <li>• Pelo menos, trimestralmente</li> <li>• Após alterações significativas ao ambiente no escopo</li> </ul> <p><b>A3.2.1.b</b> Analise os resultados documentados das revisões trimestrais no escopo para verificar se os seguintes procedimentos são realizados:</p> <ul style="list-style-type: none"> <li>• Identificação de todas as redes no escopo e componentes do sistema</li> <li>• Identificação de todas as redes fora do escopo e justificativa para tanto, incluindo descrições de todos os controles de segmentação implementados</li> <li>• Identificação de todas as entidades conectadas — p. ex., entidades de terceiros com acesso ao CDE</li> </ul>	<p>A validação do escopo do PCI DSS deve ser executada sempre que possível, para garantir que o escopo do PCI DSS permaneça atualizado e alinhado às mudanças nos objetivos comerciais.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.2</b> Determinar o impacto do escopo do PCI DSS para todas as alterações nos sistemas ou redes, inclusive acréscimos de novos sistemas e novas conexões de rede. Os processos devem incluir:</p> <ul style="list-style-type: none"> <li>• Realização de uma avaliação de impacto formal do PCI DSS</li> <li>• Identificação dos requisitos do PCI DSS aplicáveis ao sistema ou à rede</li> <li>• Atualização do escopo do PCI DSS, conforme apropriado</li> <li>• Assinatura documentada dos resultados da avaliação de impacto pelo pessoal responsável (conforme definição na seção A3.1.3)</li> </ul> <p><b>Referência do PCI DSS:</b> Escopo dos requisitos do PCI DSS; Requisitos 1 a 12</p>	<p><b>A3.2.2</b> Analise a documentação de alteração e converse com o pessoal para verificar se, para cada mudança nos sistemas ou redes:</p> <ul style="list-style-type: none"> <li>• Foi realizada uma avaliação de impacto formal do PCI DSS.</li> <li>• Os requisitos do PCI DSS aplicáveis às mudanças no sistema ou na rede foram identificados.</li> <li>• O escopo do PCI DSS foi atualizado conforme apropriado à mudança.</li> <li>• A assinatura do pessoal responsável (conforme definição na seção A3.1.3) foi obtida e documentada.</li> </ul>	<p>Alterações aos sistemas ou redes podem gerar impacto significativo ao escopo do PCI DSS. Por exemplo, mudanças de regra no firewall podem trazer segmentos de toda a rede para o escopo ou novos sistemas podem ser adicionados ao CDE, os quais devem ser protegidos adequadamente.</p> <p>Os processos para determinar o impacto potencial que as mudanças aos sistemas e redes podem gerar no âmbito do PCI DSS da entidade podem ser realizados como parte de um programa dedicado de conformidade do PCI DSS ou podem integrar um programa principal de conformidade e/ou governança.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.2.1</b> Após concluir uma mudança, todos os requisitos relevantes do PCI DSS devem ser verificados em todas as redes e sistemas novos ou alterados; a documentação deve ser atualizada, conforme aplicável. Exemplos de requisitos do PCI DSS que devem ser verificados incluem, entre outros:</p> <ul style="list-style-type: none"> <li>▪ Diagrama da rede atualizado para refletir as mudanças.</li> <li>▪ Sistemas configurados segundo os padrões de configuração, com todas as senhas padrão alteradas e serviços desnecessários desabilitados.</li> <li>▪ Sistemas protegidos com controles necessários — p. ex., monitoramento de integridade de arquivos (FIM), antivírus, patches e registro de auditoria.</li> <li>▪ Verifique se os dados de autenticação confidenciais (SAD) não são armazenados e se todos os dados armazenados de titulares de cartão (CHD) são documentados e incorporados conforme os procedimentos e a política de retenção de dados</li> <li>▪ Novos sistemas são incluídos no processo trimestral de verificação de vulnerabilidade.</li> </ul> <p><b>Referência do PCI DSS:</b> Escopo dos requisitos do PCI DSS; Requisitos 1 a 12</p>	<p><b>A3.2.2.1</b> Para obter uma amostra das alterações nos sistemas e redes, analise os registros de mudança, converse com a equipe e observe os sistemas/redes afetados para verificar se, como parte da mudança, os requisitos referentes ao PCI DSS foram implementados e a documentação, atualizada.</p>	<p>É importante estabelecer processos para analisar todas as mudanças realizadas, a fim de garantir que todos os controles apropriados do PCI DSS serão aplicados em todas as redes ou sistemas adicionados ao ambiente do escopo, em razão da mudança.</p> <p>Estruturar a validação sobre processos de gestão de mudanças contribui para garantir que os padrões de configuração e inventários do dispositivo estejam sempre atualizados e os controles de segurança sejam aplicados onde necessário.</p> <p>O processo de gestão de mudanças deve incluir evidências capazes de comprovar que os requisitos do PCI DSS estejam implementados ou preservados através do processo iterativo.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.3</b> Mudanças na estrutura organizacional — por exemplo, fusão ou aquisição corporativa, alteração ou reatribuição de pessoal responsável pelos controles de segurança — implicam em revisão formal (interna) do impacto ao escopo do PCI DSS e aplicabilidade dos controles.</p> <p><b>Referência do PCI DSS:</b> <i>Requisito 12</i></p>	<p><b>A3.2.3</b> Analisar as políticas e os procedimentos para verificar se uma mudança na estrutura organizacional resulta em revisão formal do impacto ao escopo do PCI DSS e aplicabilidade dos controles.</p>	<p>A estrutura e a gestão da organização definem os requisitos e protocolo para operações seguras e eficientes. Mudanças na estrutura podem gerar efeitos negativos frente aos controles e conceitos existentes quando da realocação ou remoção de recursos anteriormente controlados pelo PCI DSS ou ganho de novas responsabilidades para as quais não há controles estabelecidos. Portanto, é importante consultar o escopo e os controles do PCI DSS quando houver mudanças para garantir que os controles permaneçam implementados e em atividade.</p>
<p><b>A3.2.4</b> Se a segmentação for utilizada, confirme o escopo do PCI DSS por meio do teste de penetração nos controles de segmentação, pelo menos, semestralmente e após quaisquer alterações aos controles/métodos de segmentação.</p> <p><b>Referência do PCI DSS:</b> <i>Requisito 11</i></p>	<p><b>A3.2.4</b> Analise os resultados do teste de penetração mais recente para verificar se:</p> <ul style="list-style-type: none"> <li>• O teste de penetração para verificação dos controles de segmentação é executado, pelo menos, semestralmente e após qualquer mudança nos métodos/controles da segmentação.</li> <li>• Os testes de penetração abrangem todos os controles/métodos de segmentação em uso.</li> <li>• Os testes de penetração verificam se os controles/métodos de segmentação são operacionais e eficientes, e se isolam todos os sistemas fora de escopo dos sistemas no CDE.</li> </ul>	<p>Se a segmentação é usada para isolar as redes no escopo das redes fora do escopo, os controles de segmentação devem ser verificados por meio do teste de penetração para confirmar se continuam a operar com eficiência e conforme esperado. Técnicas de teste de penetração devem seguir a metodologia existente de penetração, conforme especifica o Requisito 11 do PCI DSS.</p> <p>Para obter mais informações sobre testes de penetração eficientes, consulte as Informações Suplementares do PCI SSC, em <i>Orientações referentes ao teste de penetração</i>.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.5</b> Implementar uma metodologia de descoberta de dados para confirmar o escopo do PCI DSS e localizar todas as fontes e locais onde há PAN em texto simples, pelo menos, trimestralmente e após mudanças significativas aos processos ou ambiente do titular do cartão.</p> <p>A metodologia de descoberta de dados deve considerar o potencial para PAN em texto simples nos sistemas e redes fora do CDE atualmente definido.</p> <p><b>Referência do PCI DSS:</b> <i>Escopo dos requisitos do PCI DSS</i></p>	<p><b>A3.2.5.a</b> Analise a metodologia documentada de descoberta de dados para verificar o seguinte:</p> <ul style="list-style-type: none"> <li>• A metodologia de descoberta de dados considera processos para identificar todas as fontes e locais onde há PAN em texto simples.</li> <li>• A metodologia considera o potencial para PAN em texto simples nos sistemas e redes fora do CDE atualmente definido.</li> </ul> <hr/> <p><b>A3.2.5.b</b> Analise os resultados dos esforços recentes em descoberta de dados e converse com o pessoal responsável para verificar se a descoberta de dados é executada, pelo menos, trimestralmente e após mudanças significativas aos processos ou ambiente do titular do cartão.</p>	<p>O PCI DSS exige que, como parte do escopo em exercício, as entidades auditadas devem identificar e documentar todas as ocorrências de PAN em texto simples nos seus ambientes. A implementação de uma metodologia de descoberta de dados que identifica todas as fontes e locais onde há PAN em texto simples e leva em consideração o potencial para ocorrências de PAN em texto simples nos sistemas e redes fora do CDE atualmente definido ou em locais imprevisos no CDE definido — por exemplo, em um arquivo de registro de erro ou despejo de memória — ajuda a garantir que os locais anteriormente desconhecidos para PAN em texto simples sejam detectados e devidamente protegidos.</p> <p>O processo de descoberta de dados pode ser realizado através de diversos métodos, inclusive, entre outros: (1) software de descoberta de dados comercialmente disponível, (2) programa de descoberta de dados desenvolvido internamente ou (3) uma busca manual. Independentemente do método utilizado, o objetivo do esforço é encontrar todas as fontes e locais onde há PAN em texto simples (não apenas no CDE definido).</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.5.1</b> Certifique-se da eficiência dos métodos utilizados para a descoberta de dados —, p. ex., os métodos devem ser capazes de detectar PAN em texto simples em todos os tipos de componentes do sistema (por exemplo, em cada plataforma ou sistema operacional) e formatos de arquivo em uso.</p> <p>A eficiência dos métodos para descoberta de dados deve ser confirmada, pelo menos, anualmente.</p> <p><b>Referência do PCI DSS:</b> <i>Escopo dos requisitos do PCI DSS</i></p>	<p><b>A3.2.5.1.a</b> Converse com o pessoal e analise a documentação para verificar se:</p> <ul style="list-style-type: none"> <li>▪ A entidade tem um processo estabelecido para testar a eficiência dos métodos utilizados para descoberta de dados.</li> <li>▪ O processo inclui a verificação dos métodos capazes de detectar PAN em texto simples em todos os tipos de componentes do sistema e formatos de arquivo em uso.</li> </ul> <p><b>A3.2.5.1.b</b> Analise os resultados dos últimos testes de eficiência para verificar se a eficácia dos métodos utilizados na descoberta de dados é confirmada, pelo menos, anualmente.</p>	<p>Um processo para testar a eficiência dos métodos utilizados para a descoberta de dados garante a integralidade e a precisão da detecção de dados do titular do cartão. Para integridade, pelo menos uma amostra dos componentes do sistema nas redes dentro e fora do escopo deve ser incluída no processo de descoberta de dados. A precisão pode ser testada ao dispôr PANs de teste em uma amostra dos componentes do sistema e formatos de arquivo em uso e, em seguida, confirmando se o método de descoberta de dados detectou os PANs de teste.</p>
<p><b>A3.2.5.2</b> Implemente procedimentos de resposta a serem acionados quando da detecção de PAN em texto simples fora do CDE, para incluir:</p> <ul style="list-style-type: none"> <li>▪ Procedimentos para determinar as ações a serem tomadas quando da detecção de PAN em texto simples fora do CDE, inclusive recuperação, exclusão com segurança e/ou migração para o CDE atualmente definido, conforme aplicável</li> <li>▪ Procedimentos para determinar como os dados foram parar fora do CDE</li> <li>▪ Procedimentos para corrigir vazamentos de dados ou lacunas no processo que resultou na localização de dados fora do CDE</li> <li>▪ Procedimentos para identificar a fonte dos dados</li> <li>▪ Procedimentos para identificar se há caminho de dados armazenado com os PANs</li> </ul>	<p><b>A3.2.5.2.a</b> Analise os procedimentos de resposta documentados para verificar se foram definidos procedimentos de resposta para detecção de PAN em texto simples fora o CDE e se incluem:</p> <ul style="list-style-type: none"> <li>▪ Procedimentos para determinar as ações a serem tomadas quando da detecção de PAN em texto simples fora do CDE, inclusive recuperação, exclusão com segurança e/ou migração para o CDE atualmente definido, conforme aplicável</li> <li>▪ Procedimentos para determinar como os dados foram parar fora do CDE</li> <li>▪ Procedimentos para corrigir vazamentos de dados ou lacunas no processo que resultou na localização de dados fora do CDE</li> <li>▪ Procedimentos para identificar a fonte dos dados</li> <li>▪ Procedimentos para identificar se há caminho de dados armazenado com os PANs</li> </ul> <p><b>A3.2.5.2.b</b> Converse com o pessoal e analise os registros das ações de resposta para verificar se as atividades de correção são executadas quando da</p>	<p>O estabelecimento de procedimentos de resposta documentados para serem seguidos em caso de detecção de PAN em texto simples fora do CDE contribui para identificar as ações corretivas necessárias e prevenir futuros vazamentos. Por exemplo, se houve detecção de PAN fora do CDE, deve-se proceder à análise para (1) determinar se o PAN foi salvo independentemente de outros dados (ou se integrava um caminho completo), (2) identificar a fonte dos dados e (3) identificar lacunas no controle que provocaram a localização dos dados fora do CDE.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.2.6</b> Implemente mecanismos para detectar e evitar a saída de PAN em texto simples do CDE via canais, métodos ou processos não autorizados, incluindo a geração de alertas e logs de auditoria.</p> <p><i>Referência do PCI DSS: Escopo dos requisitos do PCI DSS</i></p>	<p>detecção de PAN em texto fora do CDE.</p> <p><b>A3.2.6.a</b> Analise a documentação e observe os mecanismos implementados para verificar se os mecanismos encontram-se:</p> <ul style="list-style-type: none"> <li>• Implementados e em funcionamento</li> <li>• Configurados para detectar e evitar a saída de PAN em texto simples do CDE via canais, métodos ou processos não autorizados</li> <li>• Gerando logs e alertas sobre a detecção de PAN em texto simples deixando o CDE via canais, métodos ou processos não autorizados</li> </ul> <p><b>A3.2.6.b</b> Analise os alertas e logs de auditoria e converse com o pessoal responsável para verificar se os alertas são investigados.</p>	<p>Mecanismos para detectar e evitar a perda não autorizada de PAN em texto simples podem incluir ferramentas adequadas — como soluções de prevenção contra perda de dados (DLP) — e/ou processos e procedimentos manuais. A abrangência dos mecanismos deve considerar, entre outros, e-mails, downloads para mídia removível e saída para impressoras. O emprego dos mecanismos permite à organização detectar e evitar situações que podem resultar na perda de dados.</p>
<p><b>A3.2.6.1</b> Estabeleça procedimentos de resposta a serem iniciados após a detecção de tentativas para remoção do PAN em texto simples do CDE via canais, métodos ou processos não autorizados. Os procedimentos de resposta devem incluir:</p> <ul style="list-style-type: none"> <li>▪ Procedimentos para investigação de alertas pelo pessoal responsável, em tempo hábil</li> <li>▪ Procedimentos para correção de vazamentos de dados ou lacunas no processo, conforme necessário, para evitar a perda de dados</li> </ul>	<p><b>A3.2.6.1.a</b> Analise os procedimentos de resposta documentados para verificar se os procedimentos de resposta à tentativa de remoção do PAN em texto simples do CDE via canais, métodos ou processos não autorizados incluem:</p> <ul style="list-style-type: none"> <li>▪ Procedimentos para investigação de alertas pelo pessoal responsável, em tempo hábil</li> <li>▪ Procedimentos para correção de vazamentos de dados ou lacunas no processo, conforme necessário, para evitar a perda de dados</li> </ul> <p><b>A3.2.6.1.b</b> Converse com o pessoal e analise os registros das ações tomadas quando há detecção de PAN em texto simples saindo do CDE via canais, métodos ou processos não autorizados e verifique se foram executadas atividades de correção.</p>	<p>As tentativas de remoção do PAN em texto simples via canais, métodos ou processos não autorizados podem indicar intenção maliciosa de roubo de dados ou podem refletir as ações de um funcionário autorizado que desconhece ou simplesmente não cumpre os métodos vigentes. A investigação das ocorrências em tempo hábil contribui para identificar onde há necessidade de correções e fornece informações valiosas para ajudar a entender a origem das ameaças.</p>
<p><b>A3.3 PCI DSS validado e incorporado às atividades comerciais de rotina (BAU)</b></p>		
<p><b>A3.3.1</b> Implemente um processo para detecção imediata e alerta sobre falhas no controle de segurança crítica. São exemplos</p>	<p><b>A3.3.1.a</b> Analise as políticas e os procedimentos documentados para verificar se há processos definidos para detecção imediata e subsequente alerta</p>	<p>Se não houver processos formais para detecção e alerta (assim que possível) referente à ocorrência de falha nos controles de</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p>de controles de segurança crítica, entre outros:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivírus</li> <li>• Controles de acesso físico</li> <li>• Controles de acesso lógico</li> <li>• Mecanismos de registro de auditoria</li> <li>• Controles de segmentação (se usados)</li> </ul> <p><b>Referência do PCI DSS:</b> Requisitos 1-12</p>	<p>sobre falhas no controle de segurança crítica.</p> <p><b>A3.3.1.b</b> Analise os processos de detecção e alerta e converse com os funcionários para verificar se há processos implementados para todos os controles de segurança crítica, e se a falha de um controle de segurança crítica resulta na geração de um alerta.</p>	<p>segurança crítica, as falhas podem passar despercebidas por períodos prolongados e conferir aos invasores tempo suficiente para comprometer sistemas e roubar dados confidenciais do ambiente de dados do titular de cartão.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.3.1.1</b> Solucione falhas nos controles de segurança crítica em tempo hábil. Os processos para solucionar falhas nos controles de segurança devem incluir:</p> <ul style="list-style-type: none"> <li>▪ Restabelecimento de funções de segurança</li> <li>▪ Identificação e documentação da duração (data e hora do início ao fim) da falha de segurança</li> <li>▪ Identificar e documentar as causas de falha, incluindo a causa raiz e documentar a correção necessária para tratar da causa raiz.</li> <li>▪ Identificação e tratamento de quaisquer questões de segurança que surgiram durante a falha</li> <li>▪ Proceder à avaliação de riscos para determinar a necessidade de outras ações como resultado da falha na segurança</li> <li>▪ Implementação de controles para prevenir a causa da falha de reocorrer</li> <li>▪ Retomar o monitoramento dos controles de segurança</li> </ul> <p><b>Referência do PCI DSS:</b> Requisitos 1-12</p>	<p><b>A3.3.1.1.a</b> Analise os procedimentos e as políticas documentadas e converse com o pessoal para verificar se há processos definidos e implementados para solucionar falhas no controle de segurança que incluam:</p> <ul style="list-style-type: none"> <li>▪ Restabelecimento de funções de segurança</li> <li>▪ Identificação e documentação da duração (data e hora do início ao fim) da falha de segurança</li> <li>▪ Identificar e documentar as causas de falha, incluindo a causa raiz e documentar a correção necessária para tratar da causa raiz.</li> <li>▪ Identificação e tratamento de quaisquer questões de segurança que surgiram durante a falha</li> <li>▪ Proceder à avaliação de riscos para determinar a necessidade de outras ações como resultado da falha na segurança</li> <li>▪ Implementação de controles para prevenir a causa da falha de reocorrer</li> <li>▪ Retomar o monitoramento dos controles de segurança</li> </ul> <p><b>A3.3.1.1.b</b> Analise os registros para verificar se as falhas no controle de segurança estão documentadas e incluem:</p> <ul style="list-style-type: none"> <li>▪ Identificação das causas da falha, incluindo a causa raiz</li> <li>▪ Duração (data e hora de início e fim) da falha de segurança</li> <li>▪ Detalhes da correção necessária para solucionar a causa raiz</li> </ul>	<p>Evidências documentadas (p. ex., registros em um sistema de gerenciamento de problemas) devem conferir suporte para a existência de processos e procedimentos capazes de solucionar falhas de segurança. Além disso, o pessoal deve estar ciente de suas responsabilidades em caso de falha. Ações e respostas às falhas devem ser registradas nas evidências documentadas.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.3.2</b> Analise as tecnologias de hardware e software, pelo menos, anualmente, para confirmar se ainda atendem aos requisitos do PCI DSS da organização. (Por exemplo, uma revisão das tecnologias para as quais já não há suporte por parte do fornecedor e/ou que já não atendem às necessidades de segurança da organização).</p> <p>O processo inclui um plano para correção das tecnologias que já não atendem aos requisitos do PCI DSS da organização, considerando inclusive a substituição de tecnologias, conforme apropriado.</p> <p><b>Referência do PCI DSS:</b> Requisitos 2, 6</p>	<p><b>A3.3.2.a</b> Analise as políticas e os procedimentos documentados e converse com o pessoal para verificar se há processos definidos e implementados para revisão das tecnologias de hardware e software, com a finalidade de confirmar se continuam a atender aos requisitos do PCI DSS da organização.</p> <p><b>A3.3.2.b</b> Verifique os resultados das análises recentes para verificar se as análises ocorrem, pelo menos, anualmente.</p> <p><b>A3.3.2.c</b> Para tecnologias que já não cumprem os requisitos do PCI DSS da organização, verifique se há proposição de um plano para correção da tecnologia.</p>	<p>As tecnologias de hardware e software evoluem constantemente. As organizações devem estar cientes em relação às mudanças nas tecnologias que utilizam, bem como à evolução das ameaças frente às tecnologias em uso. As organizações também devem estar cientes das alterações feitas pelos fornecedores de tecnologia para os produtos ou processos de apoio, para compreender como as mudanças podem afetar o uso da tecnologia pela organização.</p> <p>Análises regulares das tecnologias que geram impacto ou influenciam os controles do PCI DSS podem ajudar na aquisição, uso e implementação de estratégias, além de garantir a continuidade da eficiência dos controles que dependem dessas tecnologias.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>A3.3.3</b> Proceda às análises, pelo menos, trimestralmente para verificar se as atividades BAU estão sendo cumpridas. As análises devem ser realizadas pelo pessoal designado para o programa de conformidade do PCI DSS (conforme previsto na seção A3.1.3) e incluem o seguinte:</p> <ul style="list-style-type: none"> <li>• Confirmação de que todas as atividades BAU estão sendo realizadas (p. ex., A3.2.2, A3.2.6 e A3.3.1)</li> <li>• Confirmação de que o pessoal está cumprindo as políticas de segurança e os procedimentos operacionais (por exemplo, revisões diárias de registro, revisão do conjunto de regras do firewall, padrões de configuração para novos sistemas etc.)</li> <li>• Documentar como as revisões foram concluídas, incluindo a forma como todas as atividades BAU foram verificadas e consideradas em execução.</li> <li>• Coleta de evidência documentada conforme necessário para avaliação anual do PCI DSS</li> <li>• Revisão e assinatura dos resultados pelos funcionários com atribuição de responsabilidade no programa de conformidade do PCI DSS (conforme definição na seção A3.1.3)</li> <li>• Retenção de registros e documentação referentes ao período de, pelo menos, 12 meses, com abrangência de todas as atividades BAU</li> </ul>	<p><b>A3.3.3.a</b> Analise as políticas e os procedimentos para verificar se há processos definidos para análise e verificação das atividades BAU. Verifique se os procedimentos incluem:</p> <ul style="list-style-type: none"> <li>• Confirmação de que todas as atividades BAU estão sendo realizadas (por exemplo, A3.2.2, A3.2.6 e A3.3.1)</li> <li>• Confirmação de que o pessoal está cumprindo as políticas de segurança e os procedimentos operacionais (p. ex., revisões diárias de registro, revisão do conjunto de regras do firewall, padrões de configuração para novos sistemas etc.)</li> <li>• Documentar como as revisões foram concluídas, incluindo a forma como todas as atividades BAU foram verificadas e consideradas em execução</li> <li>• Coletar evidência documentada conforme necessário para avaliação anual do PCI DSS</li> <li>• Revisão e assinatura dos resultados pela gerência executiva responsável pela governança do PCI DSS</li> <li>• Retenção dos registros e documentação referentes ao período de, pelo menos, 12 meses, com abrangência de todas as atividades BAU</li> </ul> <p><b>A3.3.3.b</b> Converse com o pessoal responsável e examine os registros das análises para verificar se:</p> <ul style="list-style-type: none"> <li>• As análises são realizados pelo pessoal designado segundo o programa de conformidade do PCI DSS</li> <li>• As revisões são realizadas, pelo menos, trimestralmente</li> </ul>	<p>A implementação de controles do PCI DSS em atividades comerciais de rotina revela-se como método eficaz para garantir a inclusão da segurança como parte das operações comerciais normais regularmente. Portanto, é importante que verificações independentes sejam executadas, para garantir que os controles das BAU estão ativos e funcionam conforme o esperado.</p> <p>A intenção das verificações independentes é analisar as evidências que confirmam se as atividades comerciais de rotina estão sendo realizadas.</p> <p>As revisões também podem ser usadas para verificar se a evidência adequada está sendo mantida (por exemplo, logs de auditoria, relatórios de varredura de vulnerabilidade, revisões do firewall etc.), a fim de auxiliar na preparação da entidade para a próxima avaliação do PCI DSS.</p>

A3 Requisitos	Procedimentos de teste	Orientação
<p><b>Referência do PCI DSS:</b> Requisitos 1-12</p>		
<p><b>A3.4 Controlar e gerenciar o acesso lógico ao ambiente de dados do titular do cartão</b></p>		
<p><b>A3.4.1</b> Verifique as contas de usuário e os privilégios de acesso aos componentes no escopo, pelo menos, a cada seis meses, para garantir que as contas de usuário e o acesso permaneçam adequados e autorizados com base na função de trabalho.</p> <p><b>Referência do PCI DSS:</b> Requisito 7</p>	<p><b>A3.4.1</b> Converse com os funcionários responsáveis e analise a documentação de suporte para verificar se:</p> <ul style="list-style-type: none"> <li>• As contas de usuário e os privilégios de acesso são revisados, pelo menos, a cada seis meses.</li> <li>• As revisões confirmam que o acesso está adequado com base na função de trabalho e que todo o acesso é autorizado.</li> </ul>	<p>Os requisitos de acesso evoluem ao longo do tempo, conforme os funcionários mudam de função ou saem da empresa, e conforme as funções de trabalho sofrem mudanças. Cabe à gerência rever, revalidar e atualizar regularmente o acesso do usuário, conforme necessário, para refletir as mudanças no quadro de pessoal, incluindo terceiros e funções de trabalho dos usuários.</p>
<p><b>A3.5 Identificar e solucionar eventos sob suspeita</b></p>		
<p><b>A3.5.1</b> Implemente uma metodologia para identificação de padrões de ataque e comportamento indesejável entre sistemas em tempo hábil — por exemplo, usando análises manuais coordenadas e/ou gerenciadas centralmente, ou ferramentas automatizadas de correlação de registros — para incluir, pelo menos, o seguinte:</p> <ul style="list-style-type: none"> <li>• Identificação de anormalidades ou atividade suspeita, conforme ocorrem</li> <li>• Emissão de alertas em tempo hábil ao pessoal responsável, referentes à detecção de atividade suspeita ou anormalidades</li> <li>• Resposta aos alertas em conformidade com os procedimentos de resposta documentados</li> </ul> <p><b>Referência do PCI DSS:</b> Requisitos 10, 12</p>	<p><b>A3.5.1.a</b> Analise a documentação e converse com o pessoal para verificar a existência de metodologia definida e implementada para identificar padrões de ataque e comportamento indesejável entre sistemas em tempo hábil, e que considere o seguinte:</p> <ul style="list-style-type: none"> <li>• Identificação de anormalidades ou atividade suspeita, conforme ocorrem</li> <li>• Emissão de alertas em tempo hábil ao pessoal responsável</li> <li>• Resposta aos alertas em conformidade com os procedimentos de resposta documentados</li> </ul> <p><b>A3.5.1.b</b> Analise os procedimentos de resposta a incidentes e converse com o pessoal responsável, para verificar se:</p> <ul style="list-style-type: none"> <li>• O pessoal de plantão recebe alertas em tempo hábil.</li> <li>• Os alertas são respondidos de acordo com os procedimentos de resposta documentados.</li> </ul>	<p>A capacidade de identificar padrões de ataque e comportamento indesejável entre sistemas é fundamental para prevenir, detectar ou minimizar o impacto relacionado ao comprometimento de dados. A presença de registros em todos os ambientes permite o monitoramento, alerta e análise completos, quando há algo errado. Determinar a causa do comprometimento é muito difícil, se não impossível, sem a existência de um processo para comprovar a informação de componentes críticos do sistema e sistemas que executam funções de segurança — como firewalls, IDS/IPS e sistemas de monitoramento de integridade de arquivos (FIM). Assim, os registros para todos os componentes críticos dos sistemas e sistemas que executam funções de segurança devem ser coletados, correlacionados e armazenados. O procedimento poderia incluir o uso de produtos de software e metodologias de serviço para</p>

<b>A3 Requisitos</b>	<b>Procedimentos de teste</b>	<b>Orientação</b>
		transmissão de análise em tempo real, alertas e relatórios — como gerenciamento de eventos e informações de segurança (SIEM), monitoramento da integridade de arquivos (FIM) ou detecção de mudança.

## Apêndice B: Controles de compensação

Os controles de compensação podem ser considerados na maioria dos requisitos do PCI DSS quando uma entidade não for capaz de atender a um requisito de forma explícita, conforme informado, devido a restrições de negócios documentadas ou técnicas legítimas, mas minimizou o risco associado ao requisito de modo suficiente por meio da implementação de outros controles, incluindo os de compensação.

Os controles de compensação devem atender aos seguintes critérios:

1. Atender a intenção e o rigor do requisito original do PCI DSS.
2. Forneça um nível semelhante de defesa ao requisito original do PCI DSS, como o controle de compensação que contrabalança o risco de modo suficiente para o qual o requisito original do PCI DSS tenha sido criado para fornecer uma defesa. (Consulte a seção *Navegando no PCI DSS* para obter informações sobre a intenção de cada requisito do PCI DSS.)
3. Esteja “acima e além” dos outros requisitos do PCI DSS. (Simplesmente estar em conformidade com outros requisitos do PCI DSS não é um controle de compensação.)

Ao utilizar o critério de avaliação “acima e além” para controles de compensação, considere o seguinte:

**Observação:** *Os itens nas alternativas a) a c) abaixo são apenas exemplos. Todos os controles de compensação devem ser analisados e validados quanto à suficiência pelo responsável pela avaliação que realiza a análise do PCI DSS. A efetividade de um controle de compensação depende das especificidades do ambiente no qual o controle está implementado, dos controles de segurança ao redor e da configuração do controle. As empresas devem estar cientes de que um determinado controle de compensação não será efetivo em todos os ambientes.*

- a) Os requisitos existentes do PCI DSS NÃO PODERÃO ser considerados como controles de compensação se já tiverem sido exigidos para o item sob análise. Por exemplo, as senhas para o acesso administrativo realizado que não utiliza console devem ser enviadas criptografadas para minimizar o risco de interceptação de senhas administrativas em texto simples. As entidades não podem usar outros requisitos de senha do PCI DSS (bloqueio de invasão, senhas complexas, etc.) para compensar a falta de senhas criptografadas, uma vez que os outros requisitos de senha não diminuem o risco de interceptação de senhas de texto simples. Além disso, os outros controles de senha já são requisitos do PCI DSS referente ao item sob análise (contas).
- b) Os requisitos existentes do PCI DSS PODEM ser considerados como controles de compensação se forem exigidos para outra área, mas não para o item sob análise. Por exemplo: a autenticação multifatorial é requisito do PCI DSS para acesso remoto. A autenticação multifatorial *a partir da rede interna* também pode ser considerada como controle de compensação para o acesso administrativo que não utiliza console quando não houver suporte para a transmissão de senhas criptografadas. A autenticação multifatorial pode ser aceita como controle de compensação, se: (1) atender ao objetivo do requisito original ao abordar o risco de interceptação de senhas administrativas em texto simples; e (2) for configurada de modo adequado e em um ambiente seguro.
- 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 for capaz de tornar os dados do titular do cartão ilegíveis de acordo com o Requisito 3.4 (por exemplo, por meio da criptografia), um controle de compensação poderia consistir de um dispositivo ou uma combinação de dispositivos, aplicativos e controles que abordam todos os itens a seguir: (1) segmentação da rede interna; (2) filtragem do endereço IP ou endereço MAC; e (3) autenticação multifatorial a partir da rede interna.

4. Ser proporcional ao risco adicional imposto pelo não cumprimento do requisito do PCI DSS

O responsável pela avaliação deve analisar os controles de compensação por completo durante cada avaliação anual do PCI DSS para validar se cada controle de compensação aborda adequadamente o risco para o qual o requisito do PCI DSS original foi elaborado, de acordo com os itens 1 a 4 acima. Para manter a conformidade, os processos e controles devem estar implementados para assegurar que os controles de compensação permaneçam efetivos após a conclusão da avaliação.

## Apêndice C: Planilha dos controles de compensação

Use esta planilha para definir os controles de compensação para qualquer requisito no qual os controles de compensação são usados para atender a um requisito do PCI DSS. Os controles de compensação também devem ser documentados no Relatório sobre Conformidade na seção do requisito do PCI DSS correspondente.

**Observação:** somente as empresas que realizaram uma análise dos riscos e têm restrições de negócios documentadas ou tecnológicas legítimas podem considerar o uso dos controles de compensação para atingir a conformidade.

### Número e definição do requisito:

	Informações necessárias	Explicação
<b>1. Restrições</b>	Liste as restrições que impossibilitam a conformidade com o requisito original.	
<b>2. Objetivo</b>	Defina o objetivo do controle original; identifique o objetivo atendido pelo controle de compensação.	
<b>3. Risco identificado</b>	Identifique qualquer risco adicional imposto pela ausência do controle original.	
<b>4. Definição dos controles de compensação</b>	Defina os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	
<b>5. Validação dos controles de compensação</b>	Defina como os controles de compensação foram validados e testados.	
<b>6. Manutenção</b>	Defina o processo e os controles implementados para manter os controles de compensação.	

## Planilha dos controles de compensação – Exemplo completo

Use esta planilha para definir os controles de compensação para qualquer requisito indicado como “implantado” via controles de compensação.

**Número do requisito:** 8.1.1 — *Todos os usuários são identificados com um ID de usuário exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do titular do cartão?*

	Informações necessárias	Explicação
<b>1. Restrições</b>	Liste as restrições que impossibilitam a conformidade com o requisito original.	<i>A empresa XYZ utiliza Servidores Unix independentes sem LDAP. Sendo assim, cada um deles requer um logon “raiz”. A empresa XYZ não pode gerenciar o logon “raiz” nem é possível registrar todas as atividades “raiz” por usuário.</i>
<b>2. Objetivo</b>	Defina o objetivo do controle original; identifique o objetivo atendido pelo controle de compensação.	<i>O objetivo de exigir logons exclusivos é duplo. Primeiro, não é considerado aceitável, da perspectiva de segurança, compartilhar credenciais de logon. Segundo, ter logons compartilhados impossibilita afirmar em definitivo quem é responsável por uma determinada ação.</i>
<b>3. Risco identificado</b>	Identifique qualquer risco adicional imposto pela ausência do controle original.	<i>O risco adicional ocorre no sistema de controle de acesso ao não assegurar que todos os usuários tenham um ID exclusivo e possam ser monitorados.</i>
<b>4. Definição dos controles de compensação</b>	Defina os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	<i>A empresa XYZ exigirá que todos os usuários façam login nos servidores com suas contas de usuário regulares e, em seguida, usem o comando “sudo” para executar comandos administrativos. O procedimento permite o uso de privilégios de conta “raiz” para execução de comandos predefinidos que são registrados via sudo no log de segurança. Desta forma, cada ação do usuário pode ser rastreada para sua conta individual, sem que a senha “raiz” seja compartilhada com os usuários.</i>
<b>5. Validação dos controles de compensação</b>	Defina como os controles de compensação foram validados e testados.	<i>A empresa XYZ demonstra ao avaliador que o comando sudo está configurado corretamente com o uso de um arquivo “sudoers”, que apenas comandos predefinidos podem ser executados por usuários específicos e que todas as atividades realizadas por indivíduos usando sudo encontram-se registradas para identificar as ações executadas individualmente com o uso de privilégios “raiz”.</i>
<b>6. Manutenção</b>	Defina o processo e os controles implementados	<i>A empresa XYZ documenta processos e procedimentos para garantir que as</i>

	para manter os controles de compensação.	<i>configurações “sudo” não sejam modificadas, alteradas ou removidas para permitir que usuários individuais executem comandos raiz sem monitoramento, identificação e registro individual.</i>
--	------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Apêndice D: Segmentação e amostragem de áreas de negócios/componentes do sistema

