



**Setor de cartões de pagamento (PCI)  
Padrão de segurança de dados do PCI  
Navegando pelo PCI DSS**

---

**Entendendo o porquê dos requisitos**

**Versão 1.2**

Outubro de 2008

## Alterações no documento

---

<i>Data</i>	<i>Versão</i>	<i>Descrição</i>
<i>1 de outubro de 2008</i>	<i>1.2</i>	<i>Alinhar o conteúdo com o novo PCI DSS v1.2 e implementar pequenas alterações observadas desde o original v1.1.</i>

## Índice

---

<b>Alterações no documento .....</b>	<b>i</b>
<b>Prefácio .....</b>	<b>iii</b>
<b>Elementos dos dados do portador do cartão e de autenticação confidenciais .....</b>	<b>1</b>
<i>Localização dos dados do portador do cartão e dos dados de autenticação confidenciais .....</i>	<i>2</i>
<i>Dados do rastro 1 vs. rastro 2 .....</i>	<i>3</i>
<b>Orientação relacionada para o Padrão de segurança de dados do PCI.....</b>	<b>4</b>
<b>Orientação para os Requisitos 1 e 2: Construa e mantenha uma rede segura.....</b>	<b>5</b>
<i>Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão .....</i>	<i>5</i>
<i>Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança .....</i>	<i>10</i>
<b>Orientação para os Requisitos 3 e 4: Proteger os dados do portador do cartão .....</b>	<b>13</b>
<i>Requisito 3: Proteger os dados armazenados do portador do cartão.....</i>	<i>13</i>
<i>Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas .....</i>	<i>19</i>
<b>Orientação para os Requisitos 5 e 6: Manter um programa de gerenciamento de vulnerabilidades .....</b>	<b>21</b>
<i>Requisito 5: Usar e atualizar regularmente o software ou programas antivírus .....</i>	<i>21</i>
<i>Requisito 6: Desenvolver e manter sistemas e aplicativos seguros .....</i>	<i>23</i>
<b>Orientação para os Requisitos 7, 8 e 9: Implementar medidas de controle de acesso rigorosas .....</b>	<b>30</b>
<i>Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios .....</i>	<i>30</i>
<i>Requisito 8: Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador .....</i>	<i>31</i>
<i>Requisito 9: Restringir o acesso físico aos dados do portador do cartão.....</i>	<i>35</i>
<b>Orientação para os Requisitos 10 e 11: Monitorar e Testar as Redes Regularmente .....</b>	<b>39</b>
<i>Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.....</i>	<i>39</i>
<i>Requisito 11: Testar regularmente os sistemas e processos de segurança .....</i>	<i>42</i>
<b>Orientação para o Requisito 12: Manter uma Política de Segurança de Informações .....</b>	<b>44</b>
<i>Requisito 12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços.....</i>	<i>44</i>
<b>Orientação para o Requisito A.1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada ....</b>	<b>49</b>
<b>Anexo A: Padrão de segurança de dados do PCI: documentos relacionados.....</b>	<b>51</b>

## Prefácio

Este documento descreve os 12 requisitos do Padrão de segurança de dados do Setor de cartões de pagamento (PCI DSS), junto com uma orientação para explicar o propósito de cada um deles. Este documento destina-se a auxiliar comerciantes, prestadores de serviço e instituições financeiras que podem desejar um entendimento mais claro do Padrão de segurança de dados do Setor de cartões de pagamento, bem como o significado específico e as intenções por trás dos requisitos detalhados para proteger os componentes do sistema (servidores, rede, aplicativos, etc.) que dão suporte aos ambientes dos dados dos portadores de cartão.

**OBSERVAÇÃO: Navegando pelo PCI DSS: Entendendo o porquê dos requisitos é somente uma orientação. Ao preencher uma avaliação on-site do PCI DSS ou um Questionário de auto-avaliação (SAQ), os Requisitos do PCI DSS dos Padrões de Segurança de Dados e os Questionários de auto-avaliação do PCI DSS v1.2 são os documentos de registro.**

Os requisitos do PCI DSS se aplicam a todos os componentes do sistema que estejam incluídos ou conectados no ambiente dos dados do portador do cartão. O ambiente de dados do portador do cartão integra a rede que possui os dados do portador do cartão ou dados de autenticação confidenciais, incluindo componentes de rede, servidores e aplicativos.

- Os componentes de rede podem incluir, mas não de forma exclusiva, firewalls, chaves, roteadores, pontos de acesso wireless, mecanismos de rede e outros mecanismos de segurança.
- Os tipos de servidor podem incluir, mas não de forma exclusiva, o seguinte: Web, banco de dados, autenticação, e-mail, proxy, NTP (network time protocol) e DNS (domain name server).
- Os aplicativos podem incluir, mas não de forma exclusiva, todos os aplicativos adquiridos e personalizados, incluindo os aplicativos internos e externos (Internet).

Uma segmentação de rede adequada, isolando os sistemas que armazenam, processam ou transmitem os dados do portador do cartão, pode reduzir o escopo do ambiente dos dados do portador do cartão. Um Assessor de Segurança Qualificado (QSA) pode auxiliar na determinação do escopo dentro do ambiente dos dados do portador do cartão, junto com orientação sobre como estreitar o escopo de uma avaliação do PCI DSS ao implementar uma segmentação de rede adequada. Para questões pertinentes ao fato de a implementação específica ser coerente com o padrão ou estar 'conforme' com um requisito específico, o PCI SSC recomenda que as empresas consultem um Assessor de Segurança Qualificado (QSA) para validar a implementação de tecnologia e processos, bem como a conformidade com o Padrão de segurança de dados do PCI. A experiência dos QSAs em trabalhar com ambientes de rede complexos é boa para proporcionar melhores práticas e orientação ao comerciante ou prestador de serviços na tentativa de conquistar conformidade. A Lista de Assessores de Segurança Qualificados do PCI SSC pode ser encontrada no seguinte endereço: [https://www.pcisecuritystandards.org/pdfs/pci\\_qsa\\_list.pdf](https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf).

## Elementos dos dados do portador do cartão e de autenticação confidenciais

A tabela a seguir ilustra os elementos comumente usados do portador 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**. Esta tabela não é detalhada, destina-se apenas a ilustrar os diferentes tipos de requisitos que se aplicam a cada elemento de dados.

Dados do portador do cartão são definidos como o número de conta principal (“PAN”, ou número do cartão de crédito) e outros dados obtidos como parte de uma transação de pagamento, incluindo os seguintes elementos de dados (veja mais detalhes abaixo, na tabela):

- PAN
- O nome do portador do cartão
- Data de vencimento
- Código de serviço
- Dados de autenticação confidenciais: (1) dados completos da tarja magnética, (2) CAV2/CVC2/CVV2/CID e (3) PINs/blocos de PIN)

O Número de conta principal (PAN) é o fator decisivo na aplicabilidade dos requisitos do PCI DSS e do PA-DSS. Se o PAN não for armazenado, processado ou transmitido, o PCI DSS e o PA-DSS não se aplicam.

	Elemento de dados	Armazenament o permitido	Proteção necessária	Req. do PCI DSS 3, 4
<b>Dados do portador do cartão</b>	Número da conta principal	Sim	Sim	Sim
	Nome do portador do cartão <sup>1</sup>	Sim	Sim <sup>1</sup>	Não
	Código de serviço <sup>1</sup>	Sim	Sim <sup>1</sup>	Não
	Data de vencimento <sup>1</sup>	Sim	Sim <sup>1</sup>	Não
<b>Dados de autenticação confidenciais<sup>2</sup></b>	Dados completos da tarja magnética <sup>3</sup>	Não	N/D	N/D
	CAV2/CVC2/CVV2/CID	Não	N/D	N/D
	PIN/Bloco de PIN	Não	N/D	N/D

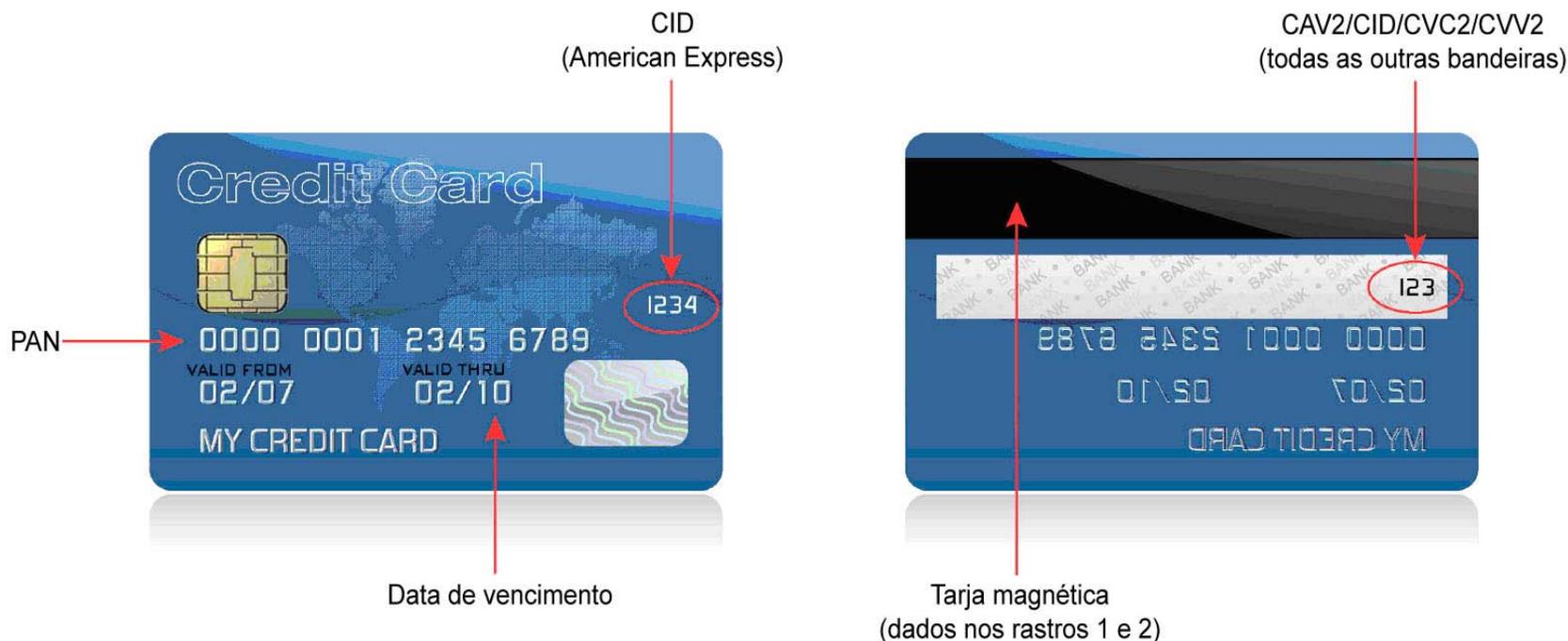
<sup>1</sup> Esses elementos de dados devem ser protegidos se forem armazenados em conjunto com o PAN. Essa proteção deve ser feita com base nos requisitos do PCI DSS para proteção geral do ambiente do portador do cartão. Além disso, outras legislações (por exemplo, relacionadas à proteção de dados do consumidor, privacidade, roubo de identidade ou segurança de dados) podem exigir uma proteção específica desses dados ou a divulgação adequada das práticas de empresas se os dados pessoais do cliente estiverem sendo coletados durante o curso dos negócios. O PCI DSS, no entanto, não se aplica se o PAN não for armazenado, processado ou transmitido.

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

<sup>3</sup> Dados de acompanhamento completo da tarja magnética, imagem da tarja magnética no chip ou outro local.

## Localização dos dados do portador do cartão e dos dados de autenticação confidenciais

Os dados de autenticação confidenciais são formados por dados da tarja magnética<sup>4</sup>, código ou valor de validação do cartão<sup>5</sup> e dados do PIN<sup>6</sup>. **O armazenamento de dados de autenticação confidenciais é proibido!** Esses dados são muito valiosos para indivíduos mal-intencionados, pois permitem gerar cartões de pagamento falsos e criar transações fraudulentas. Veja *Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS* para obter a definição completa de “dados de autenticação confidenciais”. As figuras atrás e na frente de um cartão de crédito abaixo mostram o local dos dados do portador do cartão e dos dados de autenticação confidenciais.



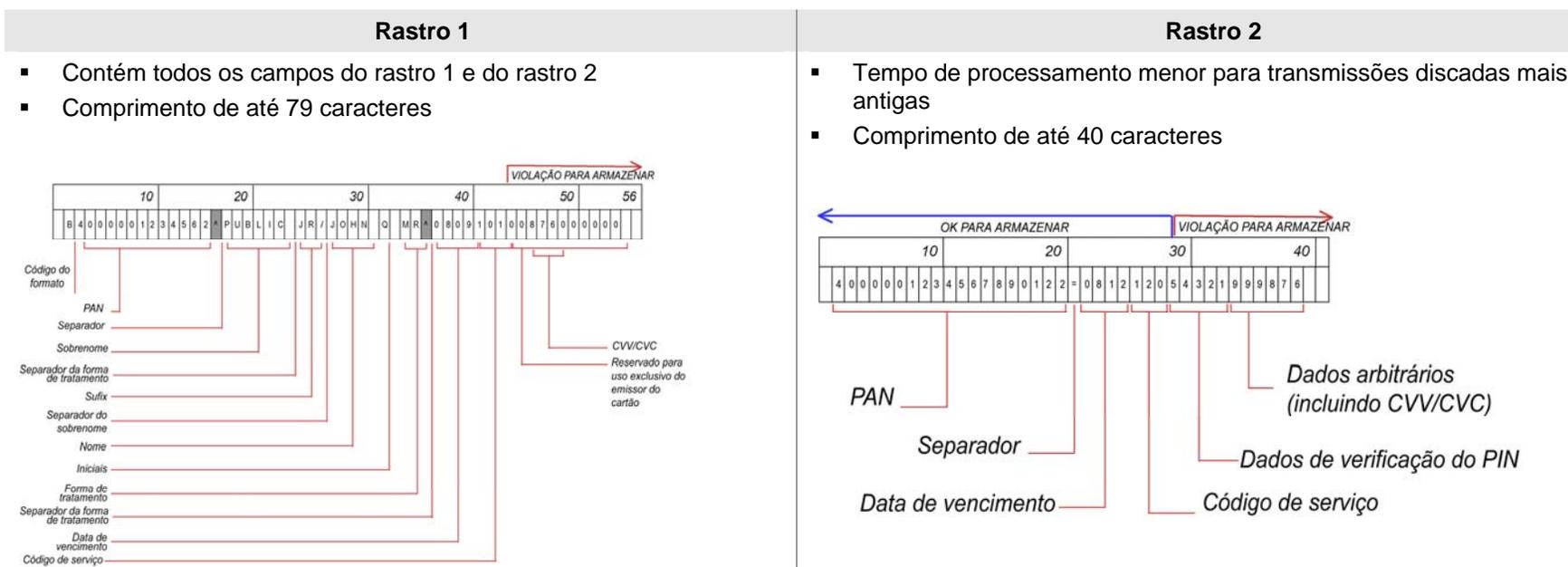
<sup>4</sup> Dados codificados na fita magnética utilizados para autorização durante a transação com o cartão. Esses dados também podem ser encontrados na imagem da tarja magnética no chip ou em algum outro lugar do cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados da tarja que podem ser retidos são o número da conta principal, o nome do portador do cartão, a data de vencimento e o código de serviço.

<sup>5</sup> O valor de três ou quatro dígitos impressos à direita do painel de assinatura ou na frente do cartão de pagamento usado para verificar transações com cartão não presente.

<sup>6</sup> Número de identificação pessoal inserido pelo portador do cartão durante uma transação com o cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

## Dados do rastro 1 vs. rastro 2

Se os dados completos de uma tarja (seja Rastro 1 ou Rastro 2, da tarja magnética, imagem da tarja magnética no chip ou outro local) forem armazenados, indivíduos mal-intencionados que obterem esses dados poderão reproduzir e vender cartões de pagamento no mundo inteiro. O armazenamento de dados completos da tarja também viola as regras operacionais das bandeiras, podendo ocasionar multas e penalidades. A ilustração abaixo fornece informações sobre os dados das Tarjas 1 e 2, descrevendo as diferenças e mostrando o layout dos dados conforme eles são armazenados na tarja magnética.



## Orientação relacionada para o Padrão de segurança de dados do PCI

### Construa e mantenha uma rede segura

---

- Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão  
Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança

### Proteger os dados do portador do cartão

---

- Requisito 3: Proteger os dados armazenados do portador do cartão  
Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas

### Manter um programa de gerenciamento de vulnerabilidades

---

- Requisito 5: Usar e atualizar regularmente o software antivírus  
Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

### Implementar medidas de controle de acesso rigorosas

---

- Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios  
Requisito 8: Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador  
Requisito 9: Restringir o acesso físico aos dados do portador do cartão

### Monitorar e Testar as Redes Regularmente

---

- Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão  
Requisito 11: Testar regularmente os sistemas e processos de segurança

### Manter uma Política de Segurança de Informações

---

- Requisito 12: Manter uma política que aborde a segurança das informações

## Orientação para os Requisitos 1 e 2: Construa e mantenha uma rede segura

### **Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do portador 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 portador 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 wireless 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.*

Requisito	Orientação
<p><b>1.1</b> Definir os padrões de configuração do firewall e do roteador que incluam o seguinte:</p>	<p>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. Sem políticas e procedimentos para documentar como a equipe deve configurar firewalls e roteadores, fica fácil uma empresa perder sua primeira linha de defesa na proteção de dados. As políticas e os procedimentos ajudarão a garantir que a primeira linha de defesa da organização na proteção de seus dados continue forte.</p>
<p><b>1.1.1</b> Processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador</p>	<p>Uma política e um processo 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.</p>
<p><b>1.1.2</b> Diagrama da rede atual com todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes wireless</p>	<p>Os diagramas de rede permitem que a organização identifique o local de todos os dispositivos de rede. Além disso, o diagrama de rede pode ser usado para mapear o fluxo de dados dos dados do portador do cartão por toda a rede e entre cada dispositivo, a fim de entender totalmente o escopo do ambiente dos dados do portador do cartão. Sem os diagramas da rede atual e do fluxo de dados, os dispositivos com dados do portador do cartão podem ser ignorados e sem querer deixados de fora dos controles de segurança em camadas implementados para PCI DSS e, assim, vulneráveis ao comprometimento.</p>

Requisito	Orientação
<p><b>1.1.3</b> Requisitos para um firewall em cada conexão da Internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna</p>	<p>Usar um firewall e todas as conexões que entram e saem da rede permite que a organização monitore e controle a entrada e saída de acesso, e minimize as chances de um indivíduo mal-intencionado de obter acesso à rede interna.</p>
<p><b>1.1.4</b> Descrição de grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede</p>	<p>Essa descrição de funções e a atribuição da responsabilidade garante que alguém seja claramente responsável pela segurança de todos os componentes e esteja ciente da responsabilidade, e também que nenhum dispositivo fique sem gerenciamento.</p>
<p><b>1.1.5</b> Documentação e justificativa comercial para o uso de todos os serviços, protocolos e portas permitidas, incluindo a documentação dos recursos de segurança implementados para os protocolos considerados inseguros</p>	<p>Muitas vezes ocorrem comprometimentos decorrentes de serviços e portas não utilizados ou inseguros, visto que é freqüente eles possuírem vulnerabilidades conhecidas – e muitas organizações estão vulneráveis a esses tipos de comprometimentos, pois não aplicam patches nas vulnerabilidades de segurança para serviços, protocolos e portas que não utilizam (ainda que as vulnerabilidades ainda estejam presentes). Cada organização deve decidir claramente quais serviços, protocolos e portas são necessários para seus negócios, documentá-los nos registros e garantir que todos os outros serviços, protocolos e portas sejam desabilitados ou removidos. Além disso, as organizações devem pensar em bloquear todo o tráfego e somente reabrir essas portas depois de ser determinada e documentada uma necessidade.</p> <p>Além disso, existem muitos serviços, protocolos ou portas de que uma empresa pode precisar (ou estarem ativados por padrão) que normalmente sejam usados por indivíduos mal-intencionados para comprometer uma rede. Se esses serviços, protocolos e portas inseguros 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, protocolos ou portas inseguros não forem necessários para a empresa, eles deverão ser desativados ou removidos.</p>
<p><b>1.1.6</b> Requisito para analisar os conjuntos de regras do firewall e do roteador 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 só permitam que serviços e portas não autorizados correspondam às justificativas de negócios.</p> <p>É aconselhável fazer essas análises com mais freqüência, como mensalmente, para garantir que os conjuntos de regras estejam atualizados e correspondam às necessidades da empresa, sem abrir furos na segurança e correr riscos desnecessários.</p>

Requisito	Orientação
<p><b>1.2</b> Elaborar uma configuração do firewall que restrinja as conexões entre redes não confiáveis e quaisquer componentes do sistema no ambiente de dados do portador do cartão.</p> <p><i>Observação: 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.</i></p>	<p>É essencial instalar proteção de rede, mais especificamente um firewall, entre a rede interna e confiável e qualquer outra rede não confiável que seja externa e/ou fique fora da capacidade de controle ou gerenciamento da entidade. A não-implementação dessa medida corretamente significa que a entidade estará vulnerável ao acesso não autorizado de indivíduos ou softwares mal-intencionados.</p> <p>Se o firewall estiver instalado, mas não tiver regras que controlam ou limitam determinado tráfego, indivíduos mal-intencionados ainda poderão explorar os protocolos e portas vulneráveis para atacar sua rede.</p>
<p><b>1.2.1</b> Restringir o tráfego de entrada e saída para aquele que é necessário para o ambiente de dados do portador do cartão</p>	<p>Esse requisito destina-se a evitar que indivíduos mal-intencionados acessem a rede da empresa por meio de endereços IP não autorizados ou usem serviços, protocolos ou portas de forma não autorizada (por exemplo, enviando dados obtidos dentro da sua rede para um servidor não confiável).</p> <p>Todos os firewalls devem incluir uma regra que negue todo tráfego de entrada e saída não especificamente necessário. Isso evita o surgimento de buracos inadvertidos que permitam a entrada ou saída de outros tráfegos indesejados e potencialmente prejudiciais.</p>
<p><b>1.2.2</b> Proteger e sincronizar os arquivos de configuração do roteador</p>	<p>Apesar de os arquivos de configuração de execução normalmente serem implementados com configurações seguras, os arquivos de inicialização (os roteadores só executam esses arquivos na reinicialização) podem não ser implementados com as mesmas configurações seguras, pois eles só são executados ocasionalmente. Quando o roteador for reinicializado sem as mesmas configurações seguras que as dos arquivos de configuração de execução, o resultado pode ser regras mais fracas que permitam que indivíduos mal-intencionados entrem na rede, pois os arquivos de inicialização podem não ter sido implementados com as mesmas configurações de segurança que os arquivos de configuração de execução.</p>
<p><b>1.2.3</b> Instalar firewalls de perímetro entre quaisquer redes wireless e o ambiente de dados do portador do cartão, configurando-os para recusar qualquer tráfego a partir do ambiente wireless ou para controlar qualquer tráfego (caso esse tráfego seja necessário para os fins comerciais).</p>	<p>A implementação conhecida (ou desconhecida) e a exploração da tecnologia wireless dentro de uma rede é um caminho comum para indivíduos mal-intencionados ganharem acesso à rede e aos dados do portador do cartão. Se um dispositivo wireless ou uma rede forem instalados sem o conhecimento da empresa, um indivíduo mal-intencionado pode fácil e “invisivelmente” entrar na rede. Se os firewalls não restringirem o acesso das redes wireless no ambiente do cartão de pagamento, indivíduos mal-intencionados que tiverem acesso não autorizado à rede wireless poderão se conectar facilmente ao ambiente do cartão de pagamento e comprometer as informações da conta.</p>

Requisito	Orientação
<p><b>1.3</b> Proibir o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do portador do cartão</p>	<p>O objetivo do firewall é gerenciar e controlar todas as conexões entre os sistemas públicos e os internos (especialmente aqueles que armazenam os dados do portador do cartão). Se for permitido o acesso direto entre sistemas públicos e aqueles que armazenam os dados do portador do cartão, as proteções oferecidas pelo firewall serão ignoradas e os componentes do sistema que armazenam os dados do portador do cartão poderão ser comprometidos.</p>
<p><b>1.3.1</b> Implementar uma DMZ para limitar o tráfego de entrada e saída somente aos protocolos que são necessários para o ambiente de dados do portador do cartão</p>	<p>Estes requisitos destinam-se a evitar que indivíduos mal-intencionados acessem a rede da empresa por meio de endereços IP não autorizados ou usem serviços, protocolos ou portas de forma não autorizada (por exemplo, enviando dados obtidos dentro da sua rede para um servidor externo não confiável em uma rede não confiável).</p>
<p><b>1.3.2</b> Limitar o tráfego de entrada da Internet a endereços IP na DMZ.</p>	
<p><b>1.3.3</b> Não permitir a entrada ou saída de nenhuma rota direta com relação ao tráfego entre a Internet e o ambiente de dados do portador do cartão</p>	<p>A DMZ faz parte do firewall que direciona para a Internet pública e gerencia conexões entre a Internet e os serviços internos que uma organização precisa disponibilizar para o público (como um servidor da Web). Essa é a primeira linha de defesa ao isolar e separar o tráfego que precisa se comunicar com a rede interna daquele que não precisa.</p>
<p><b>1.3.4</b> Não permitir que endereços internos sejam transmitidos via Internet na DMZ</p>	<p>Normalmente um pacote contém os endereços de IP do computador que originalmente o enviou, permitindo que os outros computadores da rede saibam de onde ele vem. Em certos casos, esse endereço de IP de envio sofrerá spoofing por indivíduos mal-intencionados.</p> <p>Por exemplo: indivíduos mal-intencionados enviam um pacote com um endereço spoof, para que (a menos que seu firewall proíba) o pacote consiga entrar na sua rede pela Internet, parecendo que se trata de um tráfego interno e, portanto, legítimo. Quando o indivíduo mal-intencionado estiver dentro da sua rede, ele poderá começar a comprometer seus sistemas.</p> <p>A filtragem ingressa é uma técnica que você pode usar no seu firewall para filtrar pacotes que entram na sua rede, como, entre outras coisas, garantindo que os pacotes não sofram spoofing, parecendo que vêm de sua própria rede interna.</p> <p>Para obter mais informações sobre a filtragem de pacotes, pense em obter informações sobre uma técnica complementar chamada “filtragem egressa”.</p>
<p><b>1.3.5</b> Restringir o tráfego de saída do ambiente de dados do portador do cartão à Internet de forma que o tráfego de saída possa acessar somente endereços de IP na DMZ</p>	<p>A DMZ também deve avaliar todo o tráfego de saída de dentro da rede para garantir que ele siga as regras estabelecidas. Para a DMZ servir essa função com eficácia, as conexões de dentro da rede para quaisquer endereços de fora da rede não deverão ser permitidas, a menos que primeiro sejam analisadas e avaliadas quanto à legitimidade pela DMZ.</p>

Requisito	Orientação
<p><b>1.3.6</b> Implementar inspeção com status, também conhecida como filtragem de pacote dinâmico (ou seja, somente conexões "estabelecidas" são permitidas na rede)</p>	<p>Um firewall que executa inspeção de pacotes com status mantém o "status" (ou estado) de cada conexão para o firewall. Ao manter o "status", o firewall sabe se o que parece ser uma resposta a uma conexão anterior é de fato uma resposta (visto que isso "lembra" a conexão anterior) ou se trata-se de um indivíduo ou software mal-intencionado tentando fazer spoofing ou enganar o firewall para permitir a conexão</p>
<p><b>1.3.7</b> Posicionar o banco de dados em uma zona da rede interna, separada da DMZ</p>	<p>Os dados do portador do cartão exigem o mais alto nível de proteção de informações. Se os dados do portador do cartão estiverem localizados dentro da DMZ, o acesso a essas informações será mais fácil para um atacante externo, pois há poucas camadas a serem penetradas.</p>
<p><b>1.3.8</b> Implementar o mascaramento de IP para impedir que endereços internos sejam traduzidos e revelados na Internet, usando o espaço de endereço RFC 1918. Usar as tecnologias NAT (<i>network address translation</i>)—por exemplo, PAT (<i>port address translation</i>)</p>	<p>O mascaramento de IP, que é gerenciado pelo firewall, permite que a organização tenha endereços internos que só sejam visíveis dentro da rede, e um endereço externo que seja visível externamente. Se o firewall não "ocultar" (ou mascarar) os endereços de IP da rede interna, um indivíduo mal-intencionado pode descobrir os endereços de IP internos e tentar acessar a rede com um endereço de IP obtido por spoofing.</p>
<p><b>1.4</b> Instalar o software de firewall pessoal em quaisquer computadores móveis e/ou de propriedade do funcionário com conectividade direta à Internet (por exemplo, laptops usados pelos funcionários) que sejam usados para acessar a rede da empresa</p>	<p>Se o computador não tiver instalado em si um firewall ou programa antivírus, spyware, Trojans, vírus, worms e rootkits (malware) poderão ser baixados e/ou instalados sem conhecimento. O computador fica ainda mais vulnerável quando estiver diretamente conectado à Internet, e não estiver por trás do firewall corporativo, caso em que o malware carregado em um computador poderá buscar com más intenções nas informações dentro da rede quando o computador for reconectado à rede corporativa.</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.*

Requisito	Orientação
<p><b>2.1</b> Sempre alterar os padrões disponibilizados pelo fornecedor <b>antes</b> de instalar um sistema na rede – por exemplo, incluir senhas, strings de comunidade de SNMP (<i>simple network management protocol</i>) e eliminar as contas desnecessárias</p>	<p>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 configurações são conhecidas nas comunidades de hackers e deixam seu sistema altamente vulnerável a ataques.</p>
<p><b>2.1.1</b> <b>Em ambientes wireless</b> conectados ao ambiente de dados do portador do cartão ou que transmitam dados do portador do cartão, alterar os padrões do fornecedor wireless, incluindo, mas não de forma exclusiva, chaves de criptografia wireless padrão, senhas e strings de comunidades de SNMP. Certificar-se de que as configurações de segurança do dispositivo wireless estejam ativadas com relação a uma tecnologia de criptografia robusta para a autenticação e a transmissão</p>	<p>Muitos usuários instalam esses dispositivos sem aprovação da gerência e não alteram as configurações-padrão nem fazem as configurações de segurança. Se as redes wireless não forem implementadas com configurações de segurança suficientes (incluindo a alteração das configurações-padrão), os sniffers da rede wireless conseguem espreitar o tráfego, capturar dados e senhas e entrar e atacar sua rede com facilidade. Além disso, o protocolo de troca de chaves para a versão antiga da criptografia o 802.11x (WEP) foi quebrado e pode tornar a criptografia inútil. Verifique se o firmware dos dispositivos está atualizado para suportar protocolos mais seguros, como WPA/WPA2.</p>
<p><b>2.2</b> Desenvolver padrões de configuração para todos os componentes do sistema. Certificar-se de que esses padrões abrangem todas as vulnerabilidades de segurança conhecidas e estão em conformidade com os padrões de endurecimento do sistema aceitos pelo setor</p>	<p>Existem pontos fracos conhecidos em vários sistemas operacionais, bancos de dados e aplicativos empresariais, e existem também formas conhecidas de configurar esses sistemas para corrigir as vulnerabilidades de segurança. Para ajudar quem não é especialista nisso, as organizações de segurança criaram recomendações para proteção do sistema que aconselham como corrigir esses pontos fracos. Se os sistemas forem deixados com esses pontos fracos, como por exemplo configurações de arquivo fracas ou serviços e protocolos com falhas (para aqueles serviços e protocolos que não são necessários com frequência), um transgressor poderá usar várias e conhecidas explorações para atacar serviços e protocolos vulneráveis e, assim, ganhar acesso à rede da organização. Visite esses três exemplos de sites, onde você poderá aprender mais sobre as melhores práticas da indústria que podem ajudá-lo a implementar os padrões de configuração: <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>.</p>

Requisito	Orientação
<p><b>2.2.1</b> Implementar somente uma função principal por servidor</p>	<p>Isso serve para garantir que os padrões de configuração do sistema da sua organização e os processos relacionados abordem funções do servidor que precisem ter níveis de segurança diferentes ou que possam introduzir pontos fracos de segurança em outras funções do mesmo servidor. Por exemplo:</p> <ol style="list-style-type: none"> <li>1. Um banco de dados que precise ter medidas de segurança robustas estaria arriscado a compartilhar um servidor com um aplicativo da Web, que precisa ser aberto e interagir diretamente com a Internet.</li> <li>2. A não-aplicação de um patch em uma função aparentemente pequena pode resultar em comprometimento que cause impacto em outras funções mais importantes (como um banco de dados) no mesmo servidor.</li> </ol> <p>Esse requisito vale para servidores (normalmente baseados em Unix, Linux ou Windows), mas não para sistemas de mainframe.</p>
<p><b>2.2.2</b> Desativar todos os serviços e protocolos desnecessários e inseguros (os serviços e protocolos que não precisam desempenhar diretamente a função especificada do dispositivo)</p>	<p>Conforme informado no item 1.1.7, existem muitos protocolos de que uma empresa pode precisar (ou estarem ativados por padrão) que normalmente sejam usados por indivíduos mal-intencionados para comprometer uma rede. Para garantir que esses serviços e protocolos estejam sempre desativados ao implementar novos servidores, este requisito deve fazer parte dos padrões de configuração de sua organização e dos processos relacionados.</p>
<p><b>2.2.3</b> Configurar os parâmetros de segurança do sistema para impedir o uso incorreto.</p>	<p>Isso serve para garantir que os padrões de configuração do sistema de sua organização e os processos relacionados abordem especificamente as configurações e os parâmetros de segurança que tenham implicações de segurança conhecidas.</p>
<p><b>2.2.4</b> Remover todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários.</p>	<p>Os padrões de proteção do servidor devem incluir processos para resolver funcionalidades desnecessárias com implicações de segurança específicas (como remover/desativar FTP ou o servidor da Web, caso o servidor não execute essas funções).</p>
<p><b>2.3</b> Criptografar todos os acessos administrativos não-console. Usar tecnologias como SSH, VPN ou SSL/TLS para o gerenciamento baseado na Web e outros acessos administrativos não-console.</p>	<p>Se a administração remota não for feita com autenticação segura e comunicações criptografadas, informações confidenciais de nível administrativo ou operacional (como as senhas 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>

Requisito	Orientação
<p><b>2.4</b> Os provedores de hospedagem compartilhada devem proteger cada ambiente hospedado da entidade e os dados. Esses provedores devem atender a requisitos específicos, conforme detalhado no “Anexo A: <i>Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada</i>”.</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 controle de um único ambiente, muitas vezes essas configurações nesses servidores compartilhados não serão gerenciáveis por clientes individuais, permitindo que os clientes adicionem funções e scripts inseguros 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. Veja o Anexo A.</p>

## Orientação para os Requisitos 3 e 4: Proteger os dados do portador do cartão

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

Medidas de proteção como criptografia, truncamento, mascaramento e referenciamento são componentes essenciais da proteção de dados do portador do cartão. Se um invasor burlar outros controles de segurança da rede 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 devem ser considerados como oportunidades potenciais de minimização dos riscos. Por exemplo, os métodos para minimizar os riscos incluem não armazenar os dados do portador do cartão a menos que seja absolutamente necessário, truncar os dados do portador do cartão se um PAN completo não for necessário e não enviar o PAN em e-mails não criptografados.

Consulte a seção Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter definições de "criptografia robusta" e outros termos do PCI DSS.

Requisito	Orientação
<b>3.1</b> Manter o mínimo de armazenamento de dados do portador do cartão. Desenvolver uma política de retenção e descarte de dados. Limitar a quantidade de armazenamento e o período de retenção para o que é exigido para fins comerciais, legais e/ou regulatórios, conforme documentado na política de retenção de dados.	O armazenamento prolongado dos dados do portador do cartão além das necessidades da empresa cria um risco desnecessário. Os únicos dados do portador do cartão que podem ser armazenados são o número da conta principal, ou PAN (desde que ilegível), data de vencimento, nome e código de serviço. <b>Lembre-se: se você não precisar, não os armazene!</b>
<b>3.2</b> Não armazenar dados de autenticação confidenciais após a autorização (mesmo se estiverem criptografados). Os dados de autenticação confidenciais incluem os dados conforme mencionados nos seguintes Requisitos 3.2.1 até 3.2.3.	Os dados de autenticação confidenciais são formados por dados da tarja magnética <sup>7</sup> , código ou valor de validação do cartão <sup>8</sup> e dados do PIN <sup>9</sup> . <b>O armazenamento de dados de autenticação confidenciais após a autorização é proibido!</b> Esses dados são muito valiosos para indivíduos mal-intencionados, pois permitem falsificar cartões de pagamento falsos e criar transações fraudulentas. Veja <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i> para obter a definição completa de "dados de autenticação confidenciais".

<sup>7</sup> Dados codificados na fita magnética utilizados para autorização durante a transação com o cartão. Esses dados também podem ser encontrados na imagem da tarja magnética no chip ou em algum outro lugar do cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados da tarja que podem ser retidos são o número da conta principal, o nome do portador do cartão, a data de vencimento e o código de serviço.

<sup>8</sup> O valor de três ou quatro dígitos impressos à direita do painel de assinatura ou na frente do cartão de pagamento usado para verificar transações com cartão não presente.

<sup>9</sup> Número de identificação pessoal inserido pelo portador do cartão durante uma transação com o cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

Requisito	Orientação
<p><b>3.2.1</b> Não armazenar o conteúdo completo de qualquer rastro da tarja magnética (localizada na parte posterior do cartão, em um chip ou outro local). Esses dados também são denominados como rastro completo, rastro, rastro 1, rastro 2 e dados da tarja magnética.</p> <p><i>Observação: No curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser retidos:</i></p> <ul style="list-style-type: none"> <li>▪ O nome do portador do cartão,</li> <li>▪ O número da conta principal (PAN),</li> <li>▪ A data de vencimento e</li> <li>▪ O código de serviço</li> </ul> <p><i>Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.</i></p> <p><i>Observação: Veja Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter mais informações</i></p>	<p>Se for armazenado o rastro inteiro, indivíduos mal-intencionados que obtiverem esses dados poderão reproduzir e vender cartões de pagamento em todo o mundo.</p>
<p><b>3.2.2</b> Não armazenar o código ou valor de verificação do cartão (o número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) usado para verificar as transações com cartão não presente</p> <p><i>Observação: Veja Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter mais informações</i></p>	<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. Esses tipos de transação podem ser autenticadas como originadas do proprietário do cartão somente ao solicitar esse código de validação do cartão, pois o proprietário do cartão o tem em mãos e pode ler o valor. Se esses dados proibidos forem armazenados e depois roubados, indivíduos mal-intencionados podem executar transações fraudulentas pela Internet e por MO/TO.</p>
<p><b>3.2.3</b> Não armazenar o PIN (personal identification number) ou o bloco de PIN criptografado.</p>	<p>Esses valores só devem ser conhecidos pelo proprietário do cartão ou pelo banco que emitiu o cartão. Se esses dados proibidos forem armazenados e depois roubados, indivíduos mal-intencionados podem executar transações de débito protegidas por senha (por exemplo, saques em caixas eletrônicos).</p>

Requisito	Orientação
<p><b>3.3</b> Mascaram o PAN quando exibido (os primeiros seis e quatro últimos dígitos são o número máximo de dígitos a serem exibidos).</p> <p><i>Observações:</i></p> <ul style="list-style-type: none"> <li>▪ <i>Esse requisito não se aplica aos funcionários e outras partes interessadas que precisam visualizar o PAN completo.</i></li> <li>▪ <i>Esse requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do portador do cartão – por exemplo, para recebimentos do ponto de venda (POS).</i></li> </ul>	<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. O PAN pode ser exibido em sua integridade nos recibos do tipo "cópia do comerciante"; no entanto, os recibos em papel devem obedecer aos mesmos requisitos de segurança que as cópias eletrônicas e seguir as diretrizes do Padrão de segurança de dados do PCI, especialmente o Requisito 9, sobre segurança física. O PAN completo também pode ser exibido para as pessoas com necessidade de negócios legítima de ver o PAN completo.</p>
<p><b>3.4</b> Tornar o PAN, no mínimo, ilegível em qualquer local onde ele esteja armazenado (incluindo mídia digital portátil, mídia de back-up, em registros) utilizando qualquer uma das seguintes abordagens:</p>	<p>A falta de proteção dos PANs pode permitir que indivíduos mal-intencionados visualizem ou façam download desses dados. 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. Danos decorrentes de roubo ou perda de tarjas de backup durante o transporte poderão ser reduzidos ao garantir que os PANs sejam deixados ilegíveis por meio de criptografia, truncamento ou codificação hash. Como os logs de auditoria, resolução de problemas e de exceção precisam ser retidos, você pode evitar a divulgação dos dados nos logs ao deixar os PANs ilegíveis (ou removendo-os e mascarando-os) em logs. Consulte a seção <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i> para obter definições de "criptografia robusta".</p>
<ul style="list-style-type: none"> <li>▪ Hashing de direção única com base na criptografia robusta</li> </ul>	<p>Funções de hash de direção única (como SHA-1) baseadas em uma criptografia robusta podem ser usadas para deixar os dados do portador do cartão ilegíveis. As funções de hashing são adequadas quando não houver necessidade de recuperar o número original (o hashing de direção única é irreversível).</p>
<ul style="list-style-type: none"> <li>▪ Truncamento</li> </ul>	<p>A intenção do truncamento é que somente uma parte (sem exceder os primeiros seis e os últimos quatro dígitos) do PAN seja armazenado. Isso é diferente do mascaramento, no qual o PAN inteiro é armazenado, mas isso ocorre quando ele é exibido (ou seja, somente parte do PAN é exibido em telas, relatórios, recibos, etc.).</p>
<ul style="list-style-type: none"> <li>▪ Tokens de índice e pads (os pads devem ser armazenados de forma segura)</li> </ul>	<p>Os tokens de índice e pads também podem ser usados para tornar os dados do portador do cartão ilegíveis. Um token de índice é um token criptográfico que substitui o PAN, com base em 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>

Requisito	Orientação
<ul style="list-style-type: none"> <li>▪ Criptografia robusta com processos e procedimentos de gerenciamento-chave associados</li> </ul> <p><i>As informações de conta MÍNIMAS que precisam ser convertidas como ilegíveis são o PAN.</i></p> <p><i>Observações:</i></p> <ul style="list-style-type: none"> <li>▪ <i>Se, por algum motivo, uma empresa não puder tornar o PAN ilegível, consulte o “Anexo B: Controles de compensação”.</i></li> <li>▪ <i>“Criptografia robusta” é definida em Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS.</i></li> </ul>	<p>O objetivo da criptografia robusta (veja a definição e os comprimentos da chave no documento <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 (e não um algoritmo “feito em casa”).</p>
<p><b>3.4.1</b> Se a criptografia de disco for utilizada (em vez da criptografia de bancos de dados no nível de arquivo ou coluna), o acesso lógico deve ser gerenciamento independentemente de mecanismos de controle de acesso a sistemas operacionais nativos (por exemplo, não utilizando bancos de dados de contas de usuário locais). As chaves da descrição não devem estar ligadas às contas de usuário.</p>	<p>O objetivo deste requisito é abordar a aceitabilidade da criptografia de disco para deixar os dados do portador do cartão ilegíveis. A criptografia de disco codifica os dados armazenados no armazenamento em massa do computador e descodifica automaticamente as informações quando um usuário autorizado as solicita. Os sistemas de criptografia de disco interceptam as operações de leitura e gravação do sistema operacional e executam as transformações criptográficas adequadas sem nenhuma ação especial por parte do usuário, além de fornecer uma senha ou passphrase no início de uma sessão. Com base nessas características de criptografia de disco, para obedecer a esse requisito, o método de criptografia de disco não pode ter:</p> <ol style="list-style-type: none"> <li>1) Associação direta com o sistema operacional, ou</li> <li>2) Chaves de decodificação que estejam associadas a contas de usuários.</li> </ol>
<p><b>3.5</b> Proteger as chaves criptográficas usadas para a criptografia dos dados do portador do cartão contra a divulgação e o uso incorreto:</p>	<p>As chaves criptográficas devem ser muito bem protegidas, pois quem tiver acesso a elas conseguirá decodificar os dados.</p>
<p><b>3.5.1</b> Restringir o acesso às chaves criptográficas ao menor número necessário de responsáveis pela proteção.</p>	<p>Deve haver muito poucas pessoas com acesso às chaves criptográficas, normalmente só aquelas com responsabilidades de custódia de chaves.</p>
<p><b>3.5.2</b> Armazenar chaves criptográficas de forma segura no menor número possível de locais e formatos.</p>	<p>As chaves criptográficas devem ser armazenadas em segurança, normalmente criptografadas com chaves de criptografia e armazenadas em muito poucos locais.</p>

Requisito	Orientação
<p><b>3.6</b> Documentar e implementar por completo todos os processos e procedimentos de gerenciamento-chave com relação às chaves criptográficas usadas para a criptografia dos dados do portador do cartão, incluindo 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, aborda todos os elementos de chave, de 3.6.1 a 3.6.8.</p>
<p><b>3.6.1</b> Geração de chaves criptográficas robustas</p>	<p>A solução de criptografia deve gerar chaves robustas, conforme definido em <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>, em "Criptografia robusta".</p>
<p><b>3.6.2</b> Proteger a distribuição de chaves criptográficas</p>	<p>A solução de criptografia deve distribuir as chaves de forma segura, o que significa que as chaves não deve ser distribuídas sem limitação, e sim somente para os responsáveis identificados em 3.5.1.</p>
<p><b>3.6.3</b> Proteger o armazenamento de chaves criptográficas</p>	<p>A solução de criptografia deve armazenar as chaves com segurança, o que significa que as chaves não devem ser armazenadas sem limitação (criptografe-as com uma chave de criptografia).</p>
<p><b>3.6.4</b> Alterações periódicas nas chaves criptográficas</p> <ul style="list-style-type: none"> <li>• Conforme considerado necessário e recomendado pelo aplicativo associado (por exemplo, nova atribuição de chaves); de preferência automaticamente</li> <li>• Pelo menos anualmente</li> </ul>	<p>Se oferecida pelo fornecedor do aplicativo de criptografia, siga todos os processos e recomendações do fornecedor para a troca periódica de chaves. A troca anual das chaves de criptografia é essencial para minimizar o risco de alguém obter as chaves de criptografia e conseguir decodificar os dados.</p>
<p><b>3.6.5</b> Inutilização ou substituição de chaves criptográficas comprometidas antigas ou suspeitas</p>	<p>Chaves antigas que não são mais usadas nem necessárias devem ser aposentadas e 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 (veja o item 3.6.6 abaixo). A solução de criptografia também deve levar em consideração e facilitar o processo para substituir as chaves que estejam sabidamente ou potencialmente comprometidas.</p>

Requisito	Orientação
<b>3.6.6</b> Compartilhamento do conhecimento e a determinação do controle duplo de chaves criptográficas	O conhecimento compartilhado e o controle duplo das chaves são usados para eliminar a possibilidade de uma pessoa ter acesso à chave inteira. Esse controle normalmente é aplicável para sistemas manuais de criptografia por chave, ou quando o gerenciamento de chaves não for implementado pelo produto da criptografia. Esse tipo de controle normalmente é implementado dentro dos módulos de segurança de hardware.
<b>3.6.7</b> Prevenção contra a substituição não autorizada de chaves criptográficas	A solução de criptografia não deve levar em conta nem aceitar a substituição de chaves vindas de fontes não autorizadas ou de processos inesperados.
<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 chaves.	Esse processo garante que a pessoa se comprometa com a função de responsável pela chave e entenda suas responsabilidades.

#### Requisito 4: Codificar a transmissão dos dados do portador 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 wireless configuradas de forma incorreta e vulnerabilidades na criptografia legada e protocolos de autenticação podem ser alvos contínuos de indivíduos mal-intencionados que exploram essas vulnerabilidades para obter acesso privilegiado aos ambientes de dados do portador do cartão.

Requisito	Orientação
<p><b>4.1</b> Utilizar uma criptografia robusta e protocolos de segurança como SSL/TLS ou IPSEC para proteger os dados confidenciais do portador do cartão durante a transmissão em redes abertas e públicas.</p> <p><i>Os exemplos de redes abertas e públicas que estão no escopo do PCI DSS são:</i></p> <ul style="list-style-type: none"> <li>▪ A Internet,</li> <li>▪ Tecnologias wireless,</li> <li>▪ Global System for Mobile communications (GSM), e</li> <li>▪ General Packet Radio Service (GPRS).</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. O SSL (<i>Secure Sockets Layer</i>) criptografa páginas da web e os dados inseridos nela. Ao usar sites protegidos por SSL, verifique se “https” faz parte do URL.</p> <p>Observe que as versões do SSL anteriores à v3.0 contêm vulnerabilidades documentadas, como <i>buffer overflows</i>, que um transgressor pode usar para obter controle do sistema afetado.</p>
<p><b>4.1.1</b> Certificar-se de que as redes wireless estejam transmitindo dados do portador do cartão ou estejam conectadas ao ambiente de dados do portador do cartão, usar as melhores práticas do setor (por exemplo, IEEE 802.11i) para implementar a criptografia robusta para a autenticação e a transmissão.</p> <ul style="list-style-type: none"> <li>▪ Para novas implementações wireless, será proibido implementar o WEP após 31 de março de 2009.</li> <li>▪ Para as implementações wireless atuais, será proibido implementar o WEP após 30 de junho de 2010.</li> </ul>	<p>Usuários mal-intencionados usam as várias ferramentas que estão disponíveis gratuitamente para espionar as comunicações wireless. O uso de uma criptografia adequada pode evitar essa espionagem e a revelação de informações confidenciais pela rede. Muitos comprometimentos conhecidos dos dados do portador do cartão armazenados somente em uma rede com fio foram originados quando um usuário mal-intencionado expandiu o acesso de uma rede wireless insegura.</p> <p>A criptografia robusta para autenticação e transmissão dos dados do portador do cartão é necessária para evitar que usuários mal-intencionados obtenham acesso à rede wireless – os dados na rede – ou utilizem as redes wireless para chegar a outros dados ou redes internos. O WEP não utiliza criptografia robusta. A criptografia por WEP nunca deve ser utilizada sozinha, pois é vulnerável, graças aos fracos vetores iniciais (IV) no processo de troca de chaves do WEP e à falta da rotação obrigatória de chaves. Um transgressor pode usar as ferramentas de <i>cracking</i> por força bruta amplamente disponíveis para penetrar na criptografia por WEP.</p> <p>Os atuais dispositivos wireless devem ser atualizados (por exemplo: upgrade do firmware do ponto de acesso para WPA) para dar suporte à criptografia robusta. Se os dispositivos atuais não puderem ser atualizados, devem ser adquiridos novos equipamentos.</p> <p>Se as redes wireless estiverem utilizando WEP, elas não devem ter acesso aos ambientes dos dados do portador do cartão.</p>

Requisito	Orientação
<b>4.2</b> Nunca enviar PANs não criptografados por tecnologias de envio de mensagens de usuário final (por exemplo, e-mail, sistemas de mensagens instantâneas, bate-papo).	E-mail, sistemas de mensagens instantâneas, bate-papo podem ser facilmente interceptados por sniffing de pacotes durante a entrega transversal por redes internas e públicas. Não utilize essas ferramentas de envio de mensagem para enviar o PAN se elas não tiverem recurso de criptografia.

## Orientação para os Requisitos 5 e 6: Manter um programa de gerenciamento de vulnerabilidades

### Requisito 5: Usar e atualizar regularmente o software ou programas antivírus

Softwares mal-intencionados, normalmente chamados de "malware" – incluindo vírus, worms e cavalos de Tróia – 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 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.

Requisito	Orientação
<p><b>5.1</b> Implementar softwares antivírus em todos os sistemas normalmente afetados por softwares mal-intencionados (especialmente em computadores pessoais e servidores).</p>	<p>Existe um fluxo constante de ataques usando façanhas amplamente divulgadas, muitas vezes do tipo "zero day" (publicado e divulgado por redes em até uma hora após a descoberta) contra sistemas até então seguros. Sem um software antivírus que seja atualizado regularmente, essas novas formas de software mal-intencionado podem atacar e desativar sua rede.</p> <p>Softwares mal-intencionados podem ser baixados e/ou instalados pela Internet sem você saber, mas os computadores também estão vulneráveis ao usarem dispositivos removíveis de armazenamento, como CDs e DVDs, USB memory sticks e discos rígidos, câmeras digitais, assistentes pessoais (PDAs) e outros periféricos. Sem a instalação de um software antivírus, esses computadores podem se tornar ponto de acesso para sua rede e/ou mirar nas informações dentro da rede.</p> <p>Apesar de os sistemas comumente afetados por softwares mal-intencionados normalmente não incluírem mainframes e a maioria dos sistemas Unix (veja mais detalhes abaixo), cada entidade deve ter um processo de acordo com o Requisito de PCI DSS 6.2 para identificar e resolver novas vulnerabilidade de segurança e atualizar os padrões e processos de configuração de acordo. As tendências em softwares mal-intencionados relacionadas aos sistemas operacionais que a entidade usa 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>Normalmente, os sistemas operacionais a seguir normalmente não são afetados por softwares mal-intencionados: mainframes e certos servidores Unix (como AIX, Solaris e HP-Unix). No entanto, as tendências do setor para softwares mal-intencionados podem mudar rapidamente, e cada organização deve obedecer ao Requisito 6.2 para identificar e resolver novas vulnerabilidades de segurança e atualizar os padrões e processos de configuração de acordo.</p>

Requisito	Orientação
<b>5.1.1</b> Certificar-se de que todos os programas antivírus podem detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados.	É importante proteger contra <b>TODOS</b> os tipos e formas de softwares mal-intencionados.
<b>5.2</b> Certificar-se de que todos os mecanismos antivírus estejam atualizados, funcionem ativamente e possam gerar registros de auditoria.	O melhor software antivírus tem eficácia limitada se não tiver assinaturas antivírus atualizada ou se não estiver ativo na rede ou no computador de uma pessoa. Os logs de auditoria oferecem a capacidade de monitorar a atividades do vírus e as reações do antivírus.

## 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 críticos devem contar com os patches de software adequados lançados mais recentes para proteger contra a exploração e o comprometimento dos dados do portador 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.*

Requisito	Orientação
<p><b>6.1</b> Certificar-se de que todos os componentes do sistema e softwares têm os patches de segurança mais recentes disponibilizados pelos fornecedores instalados. Instalar patches de segurança críticos em até um mês após o lançamento.</p> <p><i>Observação: Uma empresa talvez considere utilizar uma abordagem baseada nos riscos para priorizar suas instalações de patches. Por exemplo, ao priorizar mais a infra-estrutura crítica (por exemplo, dispositivos e sistemas disponibilizados ao público, bancos de dados) em vez de dispositivos internos menos críticos, para assegurar que sistemas e dispositivos de prioridade elevada sejam resolvidos em um mês e dispositivos e sistemas menos críticos em três meses.</i></p>	<p>Existe uma quantidade considerável de ataques usando façanhas amplamente divulgadas, muitas vezes do tipo “zero day” (publicadas em até uma hora) contra sistemas até então protegidos. Sem implementar os patches mais recentes nos sistemas críticos assim que possível, um indivíduo mal-intencionado pode usá-las para atacar e desativar a rede. Pense em priorizar mudanças de forma que patches de segurança críticos em sistemas essenciais ou em risco possam ser instalados em até 30 dias, e outras mudanças menos arriscadas sejam instaladas em 2-3 meses.</p>
<p><b>6.2</b> Definir um processo para identificar as vulnerabilidades de segurança descobertas recentemente (por exemplo, inscrever-se em serviços de alerta disponíveis gratuitamente na Internet). Atualizar os padrões de configuração conforme exigido pelo Requisito 2.2 do PCI DSS para solucionar novos problemas de vulnerabilidade.</p>	<p>A intenção deste requisito é que as organizações fiquem atualizadas com as novas vulnerabilidades, para que possam proteger adequadamente a rede e incorporar vulnerabilidades recém-descobertas e relevantes em seus padrões de configuração.</p>

Requisito	Orientação
<p><b>6.3</b> Desenvolver aplicativos de software de acordo com o PCI DSS (por exemplo, autenticação segura e registros) e com base nas melhores práticas do setor, além de incorporar a segurança das informações em todo o ciclo de vida do desenvolvimento dos softwares. Esses processos devem incluir o seguinte:</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 introduzidas inadvertida ou maliciosamente no ambiente de produção.</p>
<p><b>6.3.1</b> Teste de todos os patches de segurança e alterações de configuração no sistema e no software antes da implementação</p> <p><b>6.3.1.1</b> Validação de toda entrada (para impedir scripting de site cruzado, falhas na injeção, execução de arquivos maliciosos, etc.)</p> <p><b>6.3.1.2</b> Validação de manuseio de erros adequado</p> <p><b>6.3.1.3</b> Validação de armazenamento criptográfico seguro</p> <p><b>6.3.1.4</b> Validação das comunicações seguras</p> <p><b>6.3.1.5</b> Validação de controle de acesso adequado baseado na função (RBAC)</p>	<p>Garante que todas as instalações e mudanças ocorram conforme o esperado, e que elas não tenham funções que sejam inesperadas, indesejadas ou prejudiciais.</p>
<p><b>6.3.2</b> Ambientes de desenvolvimento/testes e de produção separados</p>	<p>Muitas vezes os ambientes de desenvolvimento e testes são menos protegidos que o ambiente de produção. Sem uma separação adequada, o ambiente de produção e os dados do portador do cartão podem estar arriscados por vulnerabilidades ou processos internos fracos.</p>
<p><b>6.3.3</b> Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção</p>	<p>Isso minimiza o número de funcionários com acesso ao ambiente de produção e aos dados do portador do cartão, ajudando a garantir que o acesso esteja limitado àqueles que de fato precisem desse acesso.</p>
<p><b>6.3.4</b> 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. O uso de dados de produção dá aos indivíduos mal-intencionados a oportunidade de ganhar acesso não autorizado aos dados de produção (dados do portador do cartão).</p>

Requisito	Orientação
<p><b>6.3.5</b> Remoção dos dados de teste e contas antes que os sistemas de produção tornem-se ativos</p>	<p>Dados e contas de teste devem ser removidos do código da produção antes de o aplicativo ser ativado, 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 do portador do cartão.</p>
<p><b>6.3.6</b> Remoção das contas dos aplicativos personalizados, IDs e senhas de usuários antes que os aplicativos tornem-se ativos ou sejam liberados para os clientes</p>	<p>Contas de aplicativos personalizados, IDs de usuários e senhas devem ser removidos do código da 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 do portador do cartão.</p>
<p><b>6.3.7</b> Analisar o código personalizado antes de liberar para produção ou para os clientes com o objetivo de identificar qualquer vulnerabilidade potencial de codificação.</p> <p><i>Observação: Esse requisito referente às análises dos códigos se aplica a todos os códigos personalizados (internos e voltados para o público), como parte integrante do ciclo de vida de desenvolvimento do sistema exigida pelo Requisito 6.3 do PCI DSS. As análises dos códigos podem ser realizadas por equipes internas instruídas. Os aplicativos da Web também estão sujeitos a controles extras, caso sejam voltados ao público, para abranger ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.6 do PCI DSS.</i></p>	<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 portador do cartão. Quem tiver conhecimento de técnicas de codificação seguras deve revisar o código para identificar vulnerabilidades.</p>

Requisito	Orientação
<p><b>6.4</b> Seguir os procedimentos de controle de alterações para todas as alterações nos componentes do sistema. Os procedimentos devem incluir o seguinte:</p>	<p>Sem controles de alteração de software adequados, 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. Se as políticas dos funcionários relacionados para verificações de background e controles de acesso ao sistema não forem adequadas, há um risco de indivíduos não confiáveis e sem treinamento terem acesso irrestrito ao código do software, funcionários desligados da empresa podem ter a oportunidade de comprometer sistemas e ações não autorizadas não poderão ser detectadas.</p>
<p><b>6.4.1</b> Documentação de impacto.</p>	<p>O impacto da alteração deve ser documentado de forma que todas as partes afetadas possam planejar adequadamente as mudanças de processamento.</p>
<p><b>6.4.2</b> Endosso da gerência pelas partes apropriadas.</p>	<p>A aprovação pela gerência indica que a alteração é legítima, e que a alteração autorizada foi sancionada pela organização.</p>
<p><b>6.4.3</b> Teste da funcionalidade operacional.</p>	<p>Devem ser realizados testes completos para verificar que todas as ações sejam esperadas, os relatórios sejam precisos, que todas as condições possíveis de erro reajam da forma adequada, etc.</p>
<p><b>6.4.4</b> Procedimentos de back-out</p>	<p>Para cada alteração, deve haver procedimentos de back-out in caso de falha na alteração, permitindo restaurar de volta para o estado anterior.</p>
<p><b>6.5</b> Desenvolver todos os aplicativos da Web (internos e externos, e incluindo o acesso administrativo na Web ao aplicativo) com base nas diretrizes de codificação seguras, como o <i>Guia do projeto de segurança do aplicativo aberto da Web</i>. Abranger a prevenção de vulnerabilidades de codificação comuns nos processos de desenvolvimento do software, para incluir o seguinte: <i>Observação: As vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas no guia do projeto de segurança do aplicativo aberto da Web quando a versão 1.2 do PCI DSS foi publicada. No entanto, se e quando o guia do projeto de segurança do aplicativo aberto da Web for atualizado, a versão atual deverá ser usada para esses requisitos.</i></p>	<p>A camada do aplicativo é de alto risco e pode ser almejada por ameaças internas e externas. Sem uma segurança adequada, os dados do portador do cartão e outras informações confidenciais da empresa poderão ser expostos, resultando em prejuízo à empresa, seus clientes e sua reputação.</p>

Requisito	Orientação
<p><b>6.5.1</b> Scripting de site cruzado (XSS)</p>	<p>Todos os parâmetros devem ser validados antes da inclusão. Ocorrem falhas no XSS sempre que o aplicativo pegar os dados fornecidos pelo usuário e enviá-los para um navegador sem primeiro validar ou codificar esse conteúdo. O XSS permite que os transgressores executem o script no navegador da vítima, que pode seqüestrar sessões de usuários, desfigurar sites, possivelmente introduzir worms, etc.</p>
<p><b>6.5.2</b> Falhas na injeção, particularmente na injeção SQL. Considerar também as falhas de injeção LDAP e Xpath, assim como outras falhas.</p>	<p>Valida a entrada para verificar se os dados do usuário não podem modificar o significado dos comandos e das queries. As falhas na injeção, particularmente na injeção SQL, são comuns em aplicações da Web. A injeção ocorre quando dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou query. Os dados hostis do transgressor enganam o intérprete para executar comandos não pretendidos ou para alterar os dados e permitem que o transgressor ataque os componentes dentro da rede por meio do aplicativo, a fim de iniciar ataques como buffer overflows, ou para revelar tanto informações confidenciais quando funcionalidades no aplicativo do servidor. Essa também é uma forma conhecida de fazer transações fraudulentas em sites habilitados para comércio. As informações de solicitações da web devem ser validadas antes de serem enviadas para a aplicação web – por exemplo, ao verificar todos os caracteres alfabéticos, mistura de caracteres alfabéticos e numéricos, etc.</p>
<p><b>6.5.3</b> Execução de arquivo mal-intencionado</p>	<p>Valide a entrada para verificar que o aplicativo não aceite nomes de arquivos inesperados ou arquivos de usuários. Códigos vulneráveis à inclusão de arquivos remotos (RFI) permitem que os transgressores incluam códigos e dados hostis, resultando em ataques devastadores, como comprometimento total do servidor. Os ataques de execução de arquivo mal-intencionado afetam PHP, XML e qualquer framework que aceite nomes de arquivo ou arquivos de usuários.</p>
<p><b>6.5.4</b> Referências diretas a objetos inseguros</p>	<p>Não exponha referências de objetos internos aos usuários. 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 URM ou form de parâmetro. Os transgressores podem manipular essas referências para acessar outros objetos sem autorização.</p>

Requisito	Orientação
<p><b>6.5.5</b> Falsificação de solicitações de site cruzado (CSRF)</p>	<p>Não responda a credenciais de autorização e tokens enviados automaticamente pelos navegadores. Um ataque de CSRF força o navegador da vítima logada a enviar uma solicitação pré-autenticada a um aplicativo da Web vulnerável, que então força o navegador da vítima a executar uma ação hostil em benefício do transgressor. O ataque de CSRF pode ser tão poderoso quanto o aplicativo da Web atacado.</p>
<p><b>6.5.6</b> Vazamento de informações e manuseio incorreto de erros</p>	<p>Não vaze informações por mensagens de erro ou outros meios. Os aplicativos podem sem querer vazarem informações sobre sua configuração, trabalhos internos ou violar a privacidade por meio de diversos problemas no aplicativo. Os transgressores usam esse ponto fraco para roubar dados confidenciais ou para aplicar ataques mais sérios. Além disso, o manuseio incorreto de erros fornece informações que ajudam um indivíduo mal-intencionado a comprometer o sistema. Se um indivíduo mal-intencionado puder criar erros que o aplicativo da web não conseguir 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" diz que o ID de usuário fornecido está correto e que eles devem concentrar os esforços somente na senha. Use mensagens de erro mais genéricas, como "os dados não puderam ser verificados".</p>
<p><b>6.5.7</b> Autenticação quebrada e gerenciamento de sessão</p>	<p>Autentica corretamente os usuários e protege as credenciais da conta e os tokens da sessão, que muitas vezes não são protegidos corretamente. Os transgressores comprometem senhas, chaves ou tokens de autenticação para assumir a identidades de outros usuários.</p>
<p><b>6.5.8</b> Armazenamento criptográfico seguro.</p>	<p>Evita falhas criptográficas. Os aplicativos da web raramente usam funções criptográficas propriamente para proteger dados e credenciais. Os transgressores usam dados com proteção fraca para conduzir roubo de identidade e outros crimes, como fraudes de cartão de crédito.</p>
<p><b>6.5.9</b> Comunicações inseguras.</p>	<p>Criptografe corretamente todas as comunicações autenticadas e confidenciais. Os aplicativos muitas vezes deixam de criptografar o tráfego de rede quando é necessário proteger comunicações confidenciais.</p>

Requisito	Orientação
<p><b>6.5.10</b> Falha em restringir o acesso a URLs</p>	<p>Força 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 transgressores podem usar esse ponto fraco para acessar e executar operações não autorizadas, acessando diretamente esses URLs.</p>
<p><b>6.6</b> Para aplicativos da Web voltados ao público, abordar novas ameaças e vulnerabilidades continuamente e assegurar que esses aplicativos estejam protegidos contra ataques conhecidos por <i>qualquer um</i> 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> <li>▪ Instalar um firewall para aplicativos da Web diante de aplicativos da Web voltados ao público</li> </ul>	<p>Ataques em aplicativos na Web são comuns e muitas vezes bem-sucedidos, e são permitidos por práticas de codificação ruins. Este requisito para analisar aplicativos ou instalar firewalls de aplicativos da Web destina-se a reduzir enormemente o número de comprometimentos em aplicativos da Web que resultam em violações nos dados do portador do cartão.</p> <ul style="list-style-type: none"> <li>▪ Ferramentas ou métodos de avaliação da segurança de vulnerabilidade manual ou automatizada e/ou varredura de vulnerabilidades do aplicativo podem ser usados para satisfazer este requisito.</li> <li>▪ Firewalls de aplicativo da Web filtram e bloqueiam tráfego não essencial na camada do aplicativo. Utilizado em conjunto com um firewall baseado em rede, um firewall de aplicativo da Web configurado corretamente evita ataques na camada de aplicativos caso estes estejam codificados ou configurados incorretamente.</li> </ul> <p><i>Veja Suplemento de Informações: Esclarecimento de Firewalls de Aplicativos e Revisões do Código do Requisito 6.6</i> (<a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a>) para obter mais informações.</p>

## Orientação para os Requisitos 7, 8 e 9: Implementar medidas de controle de acesso rigorosas

### **Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios**

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.

Requisito	Orientação
<p><b>7.1</b> Limitar o acesso aos componentes do sistema e aos dados do portador do cartão somente àquelas pessoas cuja função requer tal acesso. As limitações de acesso devem incluir o seguinte:</p> <p><b>7.1.1</b> Restrição dos direitos de acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função</p> <p><b>7.1.2</b> A concessão dos privilégios está baseada na classificação e na atribuição da função da equipe individual</p> <p><b>7.1.3</b> O requisito de um formulário de autorização assinado pela gerência que especifica os privilégios exigidos</p> <p><b>7.1.4</b> Implementação de um sistema de controle de acesso automático</p>	<p>Quanto mais pessoas tiverem acesso aos dados do portador do cartão, mais risco haverá de que a conta do usuário seja utilizada indevidamente. Limitar o acesso àquelas pessoas com um forte motivo corporativo para ter esse acesso ajuda sua organização a evitar o mau uso dos dados do portador do cartão por meio de inexperiência ou más intenções. Quando os direitos de acesso são concedidos somente para uma menor quantidade de dados e privilégios necessários para executar um trabalho, isso se chama "necessidade de divulgação", e quando os privilégios são atribuídos aos indivíduos com base na classificação do cargo e na função, isso se chama "controle de acesso adequado baseado na função" ou RBAC. Sua organização deve criar políticas e processos claros para controle de acesso de dados com base em "necessidade de divulgação" e usar "controle de acesso adequado baseado na função" para definir como e para quem o acesso deverá ser concedido.</p>
<p><b>7.2</b> Estabelecer um sistema de controle de acesso para os componentes do sistema com múltiplos usuários que restrinja o acesso com base na necessidade de conhecimento do usuário e esteja configurado para "recusar todos", a menos que seja permitido de forma específica. Esse sistema de controle de acesso deve incluir o seguinte:</p> <p><i>Observação: 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.</i></p> <p><b>7.2.1</b> Cobertura de todos os componentes do sistema</p> <p><b>7.2.2</b> Concessão dos privilégios às pessoas baseada na classificação e na atribuição da função</p> <p><b>7.2.3</b> Configuração padrão "recusar todos"?</p>	<p>Sem um mecanismo para restringir o acesso com base na necessidade de conhecimento do usuário, este pode sem querer receber acesso aos dados do portador do cartão. O uso de um sistema ou mecanismo de controle de acesso automatizado é essencial para gerenciar vários usuários. Esse sistema deve ser criado segundo as políticas, e os processos de controle de acesso da sua organização (incluindo "necessidade de acesso" e "controle de acesso baseado na função") devem gerenciar o acesso a todos os componentes do sistema e deve ter uma configuração padrão "recusar todos" para garantir que ninguém receba acesso até que se crie uma regra dando especificamente tal acesso.</p>

### **Requisito 8: Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador**

*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 por usuários conhecidos e autorizados, e poderão levar a eles.*

Requisito	Orientação
<p><b>8.1</b> Todos os usuários recebem um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do portador do cartão</p>	<p>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.</p>
<p><b>8.2</b> Além de atribuir um ID exclusivo, um ou mais dos seguintes métodos foi empregado para autenticar todos os usuários:</p> <ul style="list-style-type: none"> <li>▪ Senha ou passphrase</li> <li>▪ Autenticação com dois fatores (por exemplo, dispositivos de token, smart card, biométrica ou chaves públicas)</li> </ul>	<p>Esses itens de autenticação, quando usados além dos IDs exclusivos, ajuda a proteger os IDs exclusivos dos usuários contra o comprometimento (visto que quem estiver tentando o comprometimento precisa conhecer tanto o ID exclusivo quanto a senha ou outro item de autenticação).</p>
<p><b>8.3</b> Incorporar a autenticação com dois fatores ao acesso remoto (acesso no nível da rede que se origina fora dela) à rede pelos funcionários, administradores e terceiros Usar tecnologias como a autenticação remota e o serviço dial-in (RADIUS); ou sistema de controle de acesso ao controlador de acesso do terminal (TACACS) com tokens; ou VPN (baseado em SSL/TLS ou IPSEC) com certificados individuais.</p>	<p>A autenticação de dois fatores exige duas formas de autenticação para acessos com maior risco, como aqueles originados de fora de sua rede. Para uma segurança adicional, sua organização também pode considerar o uso da autenticação de dois fatores ao acessar redes de segurança mais alta a partir de redes de segurança mais baixa; por exemplo, a partir de computadores desktop corporativos (segurança mais baixa) para servidores de produção/bancos de dados com dados do portador do cartão (segurança alta).</p>
<p><b>8.4</b> Todas as senhas foram consideradas ilegíveis durante a transmissão e o armazenamento em todos os componentes do sistema que usavam criptografia robusta (definida no arquivo <i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>).</p>	<p>Muitos dispositivos de rede e aplicativos transmitem o ID do usuário e as senhas sem criptografia por uma rede e/ou também armazenam as senhas sem criptografia. Um indivíduo mal-intencionado pode facilmente interceptar o ID de usuário e a senha sem criptografia ou legível durante a transmissão usando um “sniffer”, ou então acessar diretamente os IDs do usuário e as senhas não criptografadas em arquivos onde eles são armazenados e usar esses dados roubados para obter acesso não autorizado.</p>

Requisito	Orientação
<b>8.5</b> Garantir um controle adequado da autenticação e da senha do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, da forma a seguir:	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 autenticação de usuários e gestão de senhas.
<b>8.5.1</b> Controle o acréscimo, a exclusão e a modificação dos IDs do usuário, credenciais e outros objetos do responsável pela identificação.	Para garantir que os usuários adicionados no sistema estejam sejam todos válidos e reconhecidos, a adição, exclusão e modificação dos IDs do usuário deve ser gerenciada e controlada por um pequeno grupo com autoridade específica. A capacidade de gerenciar esses IDs de usuário deve estar limitada somente a esse pequeno grupo.
<b>8.5.2</b> Verificar a identidade do usuário antes de realizar as redefinições de senha.	Muitos indivíduos mal-intencionados usam a “engenharia social” – por exemplo, ligam para o help desk e agem como um usuário legítimo – para trocar a senha, de forma que possam utilizar um ID de usuário. Pense em usar uma “pergunta secreta” que só o usuário em si possa responder para ajudar os administradores a identificarem o usuário antes de redefinir as senhas. As perguntas devem ser protegidas corretamente e não podem ser compartilhadas.
<b>8.5.3</b> Definir as senhas iniciais para um valor exclusivo para cada usuário e alterar imediatamente após a primeira utilização.	Se a mesma senha for usada para todos os novos usuários configurados, um usuário interno, ex-funcionário ou indivíduo mal-intencionado pode conhecer ou descobrir facilmente essa senha e usá-la para ter acesso às contas.
<b>8.5.4</b> Revogar imediatamente o acesso de quaisquer usuários desligados da empresa.	Se um funcionário sair da empresa e ainda tiver acesso à rede por meio de sua conta de usuário, pode ocorrer um acesso desnecessário ou mal-intencionado aos dados do portador do cartão. Esse acesso pode acontecer pelo ex-funcionário ou por um usuário mal-intencionado que explore a conta antiga e/ou não utilizada. Pense em implementar um processo com o departamento de RH para notificação imediata quando um funcionário for desligado da empresa, de forma que a conta dele possa ser rapidamente desativada.
<b>8.5.5</b> Remover/desativar as contas dos usuários inativos pelo menos a cada 90 dias.	A existência de contas inativas permite que um usuário não autorizado explore a conta não utilizada para possivelmente acessar os dados do portador do cartão.

Requisito	Orientação
<p><b>8.5.6</b> Ativar as contas usadas pelos fornecedores somente para a manutenção remota durante o período necessário.</p>	<p>Permitir que fornecedores (como os fornecedores do POS) 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. Veja também os itens 12.3.8 e 12.3.9 para saber mais sobre esse tópico.</p>
<p><b>8.5.7</b> Transmitir os procedimentos e políticas de senha a todos os usuários que têm acesso aos dados do portador do cartão.</p>	<p>Comunicar os procedimentos de senha a todos os usuários os ajuda a entender e seguir as políticas e a deixá-los alerta contra indivíduos mal-intencionados que possam tentar explorar suas senhas para obter acesso aos dados do portador do cartão (por exemplo, ligando para um funcionário e perguntando sua senha para que ele possa “resolver um problema”).</p>
<p><b>8.5.8</b> Não usar contas e senhas em grupo, compartilhadas ou genéricas.</p>	<p>Se vários usuários compartilharem a mesma conta e senha, fica impossível atribuir responsabilidade a um usuário ou fazer um registro eficaz das ações dele, pois uma determinada ação pode ter sido executada por qualquer pessoa no grupo que compartilhe da conta e da senha.</p>
<p><b>8.5.9</b> Alterar as senhas do usuário pelo menos a cada 90 dias.</p>	<p>Senhas fortes são a primeira linha de defesa para uma rede, pois um indivíduo mal-intencionado muitas vezes primeiro tentará encontrar contas com senhas fracas ou inexistentes. O indivíduo mal-intencionado terá mais tempo para localizar essas contas fracas e comprometer uma rede ao estilo de um DI de usuário válido caso as senhas seja curtas, simples de serem adivinhadas ou válidas por muito tempo sem alterações. Senhas fortes podem ser forçadas e mantidas segundo estes requisitos ao ativar os recursos de segurança de senha e de conta que vêm com o sistema operacional (como o Windows, por exemplo), redes, bancos de dados e outras plataformas.</p>
<p><b>8.5.10</b> Exigir um comprimento mínimo de senha de pelo menos sete caracteres.</p>	
<p><b>8.5.11</b> Usar senhas que contenham caracteres alfanuméricos.</p>	
<p><b>8.5.12</b> Não permitir que ninguém envie uma nova senha que seja a mesma de uma das quatro últimas senhas que tenha sido usada.</p>	
<p><b>8.5.13</b> Limitar tentativas de acesso repetidas ao bloquear o ID do usuário após seis tentativas, no máximo.</p>	<p>Sem a implementação de mecanismos de bloqueio de conta, um transgressor pode tentar continuamente adivinhar uma senha por meio de ferramentas manuais ou automatizadas (como <i>cracking</i> de senha) até ter sucesso e ganhar acesso à conta do usuário.</p>

Requisito	Orientação
<b>8.5.14</b> Definir a duração do bloqueio para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário.	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 help desk poderão validar que o proprietário da conta é a causa do bloqueio (por causa de erros de digitação).
<b>8.5.15</b> Se uma sessão estiver ociosa por mais de 15 minutos, exigir que o usuário redigite a senha para reativar o terminal.	Quando os usuários se distanciam de uma máquina aberta com acesso a dados críticos de rede e dados do portador do cartão, essa máquina poderá ser usada por outras pessoas na ausência do usuário, resultando em acesso não autorizado à conta e/ou mau uso da conta.
<b>8.5.16</b> Autenticar todos os acessos para qualquer banco de dados que contenha dados do portador do cartão, incluindo acesso por meio de aplicativos, administradores e todos os outros usuários.	Sem autenticação do usuário para acesso a bancos de dados e aplicativos, o potencial para acesso não autorizado ou malicioso 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 ter acesso direto ao banco de dados para as tarefas administrativas).

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

Qualquer acesso físico aos dados ou sistemas que armazenam dados do portador do cartão fornecem a oportunidade para as pessoas acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, e deve ser restrito de forma adequada.

Requisito	Orientação
<p><b>9.1</b> Usar controles de entrada facilitados e adequados para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do portador do cartão.</p>	<p>Sem controles de acesso físico, pessoas não autorizadas podem potencialmente ganhar acesso ao edifício e às informações confidenciais, e podem alterar as configurações do sistema, introduzir vulnerabilidades na rede ou destruir ou roubar equipamentos.</p>
<p><b>9.1.1</b> Usar câmeras de vídeo ou outros mecanismos de controle de acesso para monitorar o acesso físico individual a áreas confidenciais. Analisar os dados coletados e relacionar com outras entradas. Armazenar, por pelo menos três meses, a menos que seja restringido de outra forma pela lei.</p> <p><i>Observação: "Áreas confidenciais" referem-se a qualquer data center, sala de servidores ou qualquer área que contenha sistemas que armazenem dados do portador do cartão. Isso exclui as áreas nas quais há somente terminais do ponto de venda presentes, como as áreas dos caixas em uma loja de varejo.</i></p>	<p>Ao investigar violações físicas, esses controles podem ajudar a identificar indivíduos que acessam fisicamente as áreas que armazenam os dados do portador do cartão.</p>
<p><b>9.1.2</b> Restringir o acesso físico a pontos de rede acessíveis publicamente.</p>	<p>Restringir o acesso aos pontos de rede evita que indivíduos mal-intencionados se conectem em tomadas de rede prontamente disponíveis que pode lhes dar acesso aos recursos de rede internos. Pense em desativar as tomadas de rede enquanto elas não estiverem em uso e reativá-las somente enquanto forem necessárias. Em áreas públicas, como salas de conferência, crie redes privadas para permitir que fornecedores e visitantes acessem somente a Internet, e não sua rede interna.</p>
<p><b>9.1.3</b> Restringir o acesso físico a pontos de acesso wireless, gateways e dispositivos portáteis.</p>	<p>Sem segurança no acesso a componentes e dispositivos wireless, indivíduos mal-intencionados podem usar os dispositivos wireless da sua empresa que não estejam sendo utilizados para acessar os recursos de rede ou até para conectar seus próprios dispositivos à rede wireless, dando-lhes acesso não autorizado. Pense em colocar pontos de acesso wireless e gateways em áreas de armazenamento seguro, como dentro de armários trancados ou salas de servidores. Verifique se a criptografia robusta está ativada. Ative o bloqueio automático de dispositivo em dispositivos portáteis wireless após um período longo parado e defina uma senha nos dispositivos quando eles forem iniciados.</p>

Requisito	Orientação
<p><b>9.2</b> Desenvolver procedimentos para ajudar todas as equipes a diferenciar facilmente os funcionários dos visitantes, principalmente nas áreas onde os dados do portador do cartão podem ser acessados.</p> <p><i>Para as finalidades desse requisito, "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. Um "visitante" é definido como 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.</i></p>	<p>Sem sistemas de crachás e controles de porta, usuários não autorizados e mal-intencionados podem facilmente obter acesso às instalações para roubar, desativar, interromper ou destruir sistemas críticos e dados do portador do cartão. Para o controle ideal, pense em implementar um sistema de acesso por crachá ou carrão dentro e fora das áreas de trabalho que contenham dados do portador do cartão.</p>
<p><b>9.3</b> Certificar-se de que todos os visitantes são identificados da seguinte forma:</p>	<p>O controle de visitantes é importante para reduzir a possibilidade de pessoas não autorizadas e mal-intencionadas obterem acesso a suas instalações (e possivelmente aos dados do portador do cartão).</p>
<p><b>9.3.1</b> Autorizados antes de adentrar as áreas onde os dados do portador do cartão são processados ou mantidos.</p> <p><b>9.3.2</b> Recebem um token físico (por exemplo, um crachá ou dispositivo de acesso) que expira e que identifica os visitantes como não sendo funcionários.</p> <p><b>9.3.3</b> Devem apresentar o token físico antes de sair das dependências ou na data do vencimento.</p>	<p>Os controles de visitantes são importantes para garantir que eles só entrem em áreas onde são autorizados a tal e que sejam identificados como visitantes, de forma que os funcionários possam monitorar suas atividades e que o acesso esteja restrito a somente a duração da visita em si.</p>
<p><b>9.4</b> Usar um registro de visitantes para manter um monitoramento físico da auditoria da atividade do visitante. Documente no registro o nome do visitante, a empresa representada e o funcionário que autoriza o acesso físico. Armazene esse registro por pelo menos três meses, a menos que seja restringido de outra forma pela lei.</p>	<p>Um log de visitantes, documentando as informações mínimas sobre eles, é de manutenção fácil e barata e, durante uma possível violação de dados, ajuda a identificar acesso físico a um edifício ou a uma sala e um possível acesso aos dados do portador do cartão. Pense em implementar logs na entrada às instalações e, especialmente, em zonas onde estejam presentes os dados do portador do cartão.</p>
<p><b>9.5</b> Armazenar back-ups de mídia em um local seguro, de preferência em uma área externa, como um local alternativo ou de back-up, ou uma área de armazenamento comercial. Analisar a segurança do local pelo menos uma vez por ano.</p>	<p>Se armazenados em um local não protegido, os backups que contêm dados do portador do cartão podem ser facilmente perdidos, roubados ou copiados com más intenções. Para armazenamento protegido, pense em contratar uma empresa de armazenamento de dados comerciais OU, para empresas menores, usar um cofre em um banco.</p>

Requisito	Orientação
<b>9.6</b> Proteger fisicamente todos os documentos impressos e as mídias eletrônicas que contenham dados do portador do cartão.	Os dados do portador do cartão estarão suscetíveis a visualização, cópia ou escaneamento não autorizado caso estejam desprotegidos enquanto estiverem em mídia portátil, forem impressos ou deixados na mesa de alguém. Pense em adotar procedimentos e processos para proteger os dados do portador 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.
<b>9.7</b> Manter o controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia que contenha dados do portador do cartão, incluindo o seguinte:	
<b>9.7.1</b> Classificar a mídia para que ela possa ser identificada como confidencial.	As mídias não identificadas como confidenciais podem não ser tratadas com o cuidado necessário e podem ser perdidas ou roubadas. Inclua um processo de classificação de mídia nos procedimentos recomendados no Requisito 9.6 acima.
<b>9.7.2</b> Enviar a mídia via mensageiro seguro ou outro método de entrega que possa ser monitorado com precisão.	A mídia pode ser perdida ou roubada se for enviada por um método não rastreável, como remessa postal. Use os serviços de um mensageiro seguro para entregar mídias que contenham dados do portador do cartão, de forma que você possa usar os sistemas de rastreamento para manter inventário e localização dos envios.
<b>9.8</b> Certificar-se de que a gerência aprova quaisquer e todas as mídias contendo dados do portador do cartão que são movidas de uma área segura (principalmente quando as mídias forem distribuídas às pessoas).	Os dados do portador do cartão que saem de áreas seguras sem um processo aprovado pela gerência podem levar a dados perdidos ou roubados. Sem um processo firme, os locais de mídia não são rastreados e não existe um processo para onde os dados vão ou a forma como eles são protegidos. Inclua o desenvolvimento de um processo aprovado pela gerência para transferência de mídia nos procedimentos recomendados no Requisito 9.6 acima.
<b>9.9</b> Manter um controle rigoroso sobre o armazenamento e a acessibilidade das mídias que contenham dados do portador do cartão.	Sem métodos cuidadosos de inventário e controles de armazenamento, mídias roubadas ou ausentes podem passar despercebidas por tempo indefinido. Inclua o desenvolvimento de um processo para limitar o acesso a mídia com dados do portador do cartão nos procedimentos recomendados acima no Requisito 9.6.
<b>9.9.1</b> Manter adequadamente os registros do inventário de todas as mídias e realizar inventários das mídias pelo menos uma vez por ano.	Se a mídia não passar por inventário, mídias roubadas ou perdidas podem passar despercebidas por bastante tempo. Inclua o desenvolvimento de um processo para inventários de mídia e armazenamento seguro nos procedimentos recomendados no Requisito 9.6 acima.

Requisito	Orientação
<b>9.10</b> Destruir as mídias que contêm dados do portador do cartão quando eles não forem mais necessários por motivos de negócios ou legais, conforme se segue:	Se não forem tomadas medidas para destruir as informações contidas nos discos rígidos de computadores, em CDs e em papel, o descarte dessas informações pode resultar em comprometimento e levar a perdas financeiras ou de reputação. 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 ataque. Inclua o desenvolvimento de um processo para destruir corretamente a mídia com dados do portador do cartão, incluindo o armazenamento adequado de tais mídias antes da destruição, nos procedimentos recomendados acima no Requisito 9.6.
<b>9.10.1</b> Triturar, incinerar ou amassar materiais impressos para que os dados do portador do cartão não possam ser recuperados.	
<b>9.10.2</b> Tornar os dados do portador do cartão nas mídias eletrônicas irrecuperáveis, para que esses dados não possam ser reconstruídos.	

## Orientação para os Requisitos 10 e 11: Monitorar e Testar as Redes Regularmente

### **Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador 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 sem registros das atividades do sistema.*

Requisito	Orientação
<b>10.1</b> Definir um processo para vincular todos os acessos aos componentes do sistema (principalmente o acesso realizado com privilégios administrativos como raiz) para cada usuário individual.	É essencial ter um processo ou sistema que vincule o acesso do usuário aos componentes do sistema acessados e, mais particularmente, àqueles usuários com privilégios administrativos. Esse sistema gera logs de auditoria e oferece a capacidade de rastrear as atividades suspeitas de um usuário específico. Equipes forenses pós-incidente dependem muito desses logs para iniciar a investigação.
<b>10.2</b> Implementar trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos: <b>10.2.1</b> Todos os usuários têm acesso aos dados do portador do cartão <b>10.2.2</b> Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos <b>10.2.3</b> Acesso a todas as trilhas de auditoria <b>10.2.4</b> Tentativas de acesso lógico inválidas <b>10.2.5</b> Uso de mecanismos de identificação e autenticação <b>10.2.6</b> Inicialização dos logs de auditoria <b>10.2.7</b> Criação e exclusão de objetos do nível do sistema	Indivíduos mal-intencionados na rede muitas vezes executam várias tentativas de acesso nos sistemas alvejados. 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.

Requisito	Orientação
<p><b>10.3</b> Registrar pelo menos as seguintes entradas das trilhas de auditoria para todos os componentes do sistema para cada evento:</p> <ul style="list-style-type: none"> <li><b>10.3.1</b> Identificação do usuário</li> <li><b>10.3.2</b> Tipo de evento</li> <li><b>10.3.3</b> Data e hora</li> <li><b>10.3.4</b> Indicação de sucesso ou falha</li> <li><b>10.3.5</b> Origem do evento</li> <li><b>10.3.6</b> A identidade ou o nome dos dados afetados, componentes do sistema ou recurso</li> </ul>	<p>Ao registrar essas entradas 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 porquê.</p>
<p><b>10.4</b> Sincronizar todos os relógios e horários do sistema crítico.</p>	<p>Se um indivíduo mal-intencionado tiver entrado na rede, ele muitas vezes tentará mudar os carimbos de data e hora de suas ações dentro dos logs de auditoria para evitar a detecção da atividade. Para equipes de forenses pós-incidente, a hora de cada atividade é essencial para determinar a forma como os sistemas foram comprometidos. Um indivíduo mal-intencionado também pode tentar alterar diretamente o relógio em um servidor de hora, caso as restrições de acesso não estejam adequadas, para reconfigurar a hora para antes de ele ter entrado na rede.</p>
<p><b>10.5</b> Proteger as trilhas de auditoria para que não possam ser alteradas.</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>
<ul style="list-style-type: none"> <li><b>10.5.1</b> Limitar a exibição de trilhas de auditoria às pessoas que têm uma necessidade relacionada à função.</li> <li><b>10.5.2</b> Proteger os arquivos de trilha de auditoria de modificações não autorizadas.</li> <li><b>10.5.3</b> Fazer imediatamente o back-up dos arquivos de trilha de auditoria em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.</li> <li><b>10.5.4</b> Documentar registros quanto às tecnologias externas em um servidor de registros na LAN interna.</li> </ul>	<p>Uma proteção adequada dos logs de auditoria inclui forte controle de acesso (limitar o acesso aos logs baseado somente na “necessidade de divulgação”) e uso da segregação interna (para deixar os logs mais difíceis de serem encontrados e modificados). Ao gravar os logs de tecnologias que usam recursos externos, como wireless, 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>

Requisito	Orientação
<p><b>10.5.5</b> Usar softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos registros 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>Os sistemas de monitoramento da integridade do arquivo 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. Para arquivos de registro (que não mudam com frequência), o que deve ser monitorado é, por exemplo, quando um arquivo de log é excluído, cresce rapidamente ou diminui significativamente, e quaisquer outras indicações de que um indivíduo mal-intencionado mexeu indevidamente no arquivo de log. Existem ferramentas de prateleira e de código aberto disponíveis para monitoramento da integridade do arquivo.</p>
<p><b>10.6</b> Analisar os registros de todos os componentes do sistema pelo menos diariamente. As análises dos registros incluem aqueles servidores que desempenham funções de segurança como sistema de detecção de invasões (IDS) e servidores de protocolo de autenticação, autorização e inventário (AAA) (por exemplo, RADIUS).</p> <p><i>Observação: As ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6</i></p>	<p>Várias violações ocorrem durante dias ou meses antes de serem detectadas. A verificação diária dos logs minimiza a quantidade de tempo e exposição de uma violação em potencial. O processo de análise do log não precisa ser manual. Especialmente para as entidades com um grande número de servidores, pense em usar ferramentas de coleta, análise e alerta de log.</p>
<p><b>10.7</b> Manter um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, on-line, arquivado ou recuperável a partir do back-up).</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 tarjas de backup fora do local pode resultar em cronogramas mais longos para restaurar dados, executar análises e identificar sistemas ou dados afetados.</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.

Requisito	Orientação
<p><b>11.1</b> Testar a presença de pontos de acesso wireless usando um analisador wireless pelo menos trimestralmente ou implementando um IDS/IPS wireless para identificar todos os dispositivos wireless que estão sendo usados.</p>	<p>A implementação e/ou exploração da tecnologia wireless dentro de uma rede é um dos caminhos mais comuns para usuários mal-intencionados obterem acesso à rede e aos dados do portador do cartão. Se um dispositivo wireless ou uma rede forem instalados sem o conhecimento da empresa, ele pode permitir que um transgressor entre na rede de forma fácil e invisível. Além de analisadores wireless, podem ser usados varredores de porta e outras ferramentas de rede que detectam dispositivos wireless.</p> <p>Em função da facilidade com que o ponto de acesso wireless pode ser conectado a uma rede, da dificuldade em detectar sua presença e do risco cada vez maior apresentado por dispositivos wireless não autorizados, essas varreduras devem ser executadas até quando existir uma política proibindo o uso da tecnologia wireless.</p> <p>Uma organização deve ter, como parte de seu plano de resposta a incidentes, procedimentos documentados a serem seguidos no caso de ser detectado um ponto de acesso wireless não autorizado. Um IDS/IPS wireless deve ser configurado para gerar automaticamente um alerta, mas o plano também deve documentar procedimentos de resposta caso um dispositivo não autorizado seja detectado durante uma varredura wireless manual.</p>
<p><b>11.2</b> Executar 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, upgrades de produtos).</p> <p><i>Observação: As varreduras trimestrais quanto às vulnerabilidades externas devem ser realizadas por um Fornecedor Aprovado de Varredura (ASV) qualificado pelo Conselho de Segurança de Dados do Setor de Cartões de Pagamento (PCI SSC). As varreduras realizadas após as alterações na rede devem ser desempenhadas pela equipe interna da empresa.</i></p>	<p>Uma varredura de vulnerabilidade é uma ferramenta automatizada executada em dispositivos de rede interna e externa e servidores, feita para expor possíveis vulnerabilidades e identificar portas em redes que podem ser encontradas e exploradas por indivíduos mal-intencionados. Quando esses pontos fracos são identificados, a entidade os corrige e repete a verificação para chegar se as vulnerabilidades foram mesmo corrigidas.</p> <p>No momento da avaliação inicial do PCI DSS pela entidade, é possível que quatro varreduras trimestrais ainda não tenham sido realizadas. Se o resultado da verificação mais recente atingir os critérios para aprovação e houver políticas e procedimentos para varreduras trimestrais futuras, o objetivo desse requisito estará atingido. Caso essas condições sejam atendidas, não é necessário postergar uma avaliação “no local” para este requisito em função da falta de quatro varreduras.</p>

Requisito	Orientação
<p><b>11.3</b> Realizar testes de penetração externos e internos pelo menos uma vez por ano e após qualquer upgrade ou modificação significativa na infra-estrutura ou nos aplicativos (como um upgrade no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor da Web adicionado ao ambiente). Esses testes de penetração devem incluir o seguinte:</p> <p><b>11.3.1</b> Testes de penetração na camada de rede.</p> <p><b>11.3.2</b> Testes de penetração na camada do aplicativo.</p>	<p>Os testes de penetração na rede e no aplicativo são diferentes das varreduras de vulnerabilidade no fato de que os testes de penetração são mais manuais, tentam explorar algumas das vulnerabilidades identificadas nas varreduras e incluem técnicas usadas por indivíduos mal-intencionados para se aproveitarem dos fracos sistemas ou processos de segurança.</p> <p>Antes de os aplicativos, dispositivos de rede e sistemas serem colocados em produção, eles devem ser “endurecidos” e protegidos usando as melhores práticas de segurança (segundo o Requisito 2.2). As varreduras de vulnerabilidade e os testes de penetração devem expor todas as vulnerabilidades restantes que posteriormente poderão ser encontradas e exploradas por um transgressor.</p>
<p><b>11.4</b> Usar sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão para monitorar todo o tráfego no ambiente de dados do portador do cartão e alertar as equipes sobre comprometimentos suspeitos. Manter todos os mecanismos de detecção e prevenção contra invasões atualizados.</p>	<p>Essas ferramentas comparam o tráfego que entra na rede com “assinaturas” conhecidas 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 por meio dessas ferramentas, os ataques (ou mau uso) de recursos de computador podem passar despercebidos em tempo real. Os alertas de segurança gerados por essas ferramentas devem ser monitorados, de forma que as tentativas de intrusão possam ser interrompidas.</p> <p>Existem milhares de tipos de comprometimento, e outro tanto é descoberto diariamente. Versões antigas desses sistemas não têm as “assinaturas” atuais e não identificarão novas vulnerabilidades que poderão levar a uma violação não detectada. Os fornecedores desses produtos fornecem atualizações freqüentes, muitas vezes diárias.</p>
<p><b>11.5</b> Implementar softwares de monitoramento da integridade dos arquivos para alertar as equipes quanto à modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configurar o software para realizar comparações de arquivos críticos pelo menos semanalmente.</p> <p><i>Observação: Para fins de monitoramento da integridade dos arquivos, os arquivos críticos normalmente são aqueles que não são alterados com freqüência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Normalmente, os produtos de monitoramento da integridade dos arquivos 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).</i></p>	<p>Os sistemas de monitoramento da integridade do arquivo (FIM) verificam as alterações nos arquivos críticos e notificam quando essas alterações são detectadas. Existem ferramentas de prateleira e de código aberto disponíveis para monitoramento da integridade do arquivo. Se não implementadas corretamente e se o resultado do FIM não for monitorado, um indivíduo mal-intencionado pode alterar o conteúdo do arquivo de configuração, os programas do sistema operacional ou os executáveis do aplicativo. Essas alterações não autorizadas, se não detectadas, podem tornar os controles de segurança ineficazes e/ou resultar no roubo dos dados do portador do cartão sem impacto perceptível no processamento normal.</p>

## Orientação para o Requisito 12: Manter uma Política de Segurança de Informações

### **Requisito 12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços.**

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 desse requisito, "funcionários" 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 empresa.

Requisito	Orientação
<p><b>12.1</b> Definir, publicar, manter e disseminar uma política de segurança que realize o seguinte:</p> <p><b>12.1.1</b> Atenda a todos os requisitos do PCI DSS.</p> <p><b>12.1.2</b> Inclua um processo anual que identifica ameaças e vulnerabilidades e resulta em uma avaliação de risco formal.</p> <p><b>12.1.3</b> Inclui uma análise pelo menos uma vez por ano e atualizações quando o ambiente é modificado.</p>	<p>A política de segurança de informações de uma empresa cria um guia para implementar as medidas de segurança para proteger seus ativos mais valiosos. 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.</p> <p>As ameaças de segurança e os métodos de proteção evoluem rapidamente ao longo do ano. Sem atualizar a política de segurança para refletir essas alterações, agora são abordadas novas medidas de proteção para lutar contra essas ameaças.</p>
<p><b>12.2</b> Desenvolver procedimentos de segurança operacional diariamente que estejam em conformidade com os requisitos nessa especificação (por exemplo, procedimentos de manutenção da conta do usuário e procedimentos de análise de registros).</p>	<p>Procedimentos diários de segurança operacional agem como "instruções de mesa" para os trabalhadores usarem nas atividades diárias de manutenção e administração do sistema. Os procedimentos de segurança operacional não documentados levam a trabalhadores que não estão cientes do escopo total de suas tarefas, processos que não podem ser repetidos com facilidade por novos trabalhadores e possíveis falhas nesses processos que podem permitir que um indivíduo mal-intencionado obtenha acesso a sistemas e recursos críticos.</p>
<p><b>12.3</b> Desenvolver políticas de utilização para tecnologias críticas voltadas aos funcionários (por exemplo, tecnologias de acesso remoto, tecnologias wireless, mídia eletrônica removível, laptops, dados pessoais/assistentes digitais (PDAs), uso de e-mail e uso da Internet) para definir o uso adequado dessas tecnologias para todos os funcionários e prestadores de serviços. Assegurar que essas políticas de utilização exijam o seguinte:</p>	<p>As políticas de uso por funcionários podem ou 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 não estiverem em vigor políticas de uso, 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 portador do cartão. Um exemplo pode ser configurar sem saber redes wireless sem segurança. Para garantir que os padrões da empresa sejam seguidos e que somente as tecnologias aprovadas sejam implementadas, pense em confinar a implementação somente às equipes operacionais e não permitir que funcionários não especializados/gerais instalem essas tecnologias.</p>

Requisito	Orientação
<p><b>12.3.1</b> Aprovação explícita do gerenciamento</p>	<p>Sem exigir aprovação adequada da gestão 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>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 portador do cartão.</p>
<p><b>12.3.3</b> Uma lista de todos esses dispositivos e equipes com acesso</p>	<p>Os indivíduos mal-intencionados podem violar a segurança física e colocar seus próprios dispositivos na rede como "back door", e 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 rotule e registre todos os dispositivos de forma coerente com os controles de inventário criados.</p>
<p><b>12.3.4</b> Identificação dos dispositivos com proprietário, informações de contato e finalidade</p>	
<p><b>12.3.5</b> Usos aceitáveis das tecnologias</p>	
<p><b>12.3.6</b> Locais de rede aceitáveis para as tecnologias</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 "back door" para um indivíduo mal-intencionado obter acesso a sistemas críticos e a dados do portador do cartão.</p>
<p><b>12.3.7</b> Lista dos produtos aprovados pela empresa</p>	
<p><b>12.3.8</b> Desconexão automática das sessões para tecnologias de acesso remoto após um período específico de inatividade</p>	<p>As tecnologias de acesso remoto são freqüentes "back doors" a recursos críticos e a dados do portador do cartão. Ao desconectar as tecnologias de acesso remoto quando não estiverem em uso (por exemplo, aquelas usadas para dar suporte aos sistemas pelo POS ou por outros fornecedores), o acesso e os riscos à rede são minimizados. Pense em usar controles para desconectar dispositivos depois de 15 minutos de inatividade. Veja também o Requisito 8.5.6 para saber mais sobre esse tópico.</p>
<p><b>12.3.9</b> Ativação das tecnologias de acesso remoto para fornecedores somente quando for necessário por parte dos fornecedores, com uma desativação imediata após o uso</p>	
<p><b>12.3.10</b> Ao acessar remotamente os dados do portador do cartão por meio de tecnologias de acesso remoto, proibir a cópia, a transferência e o armazenamento dos dados do portador do cartão em discos rígidos locais e mídias eletrônicas removíveis.</p>	<p>Para garantir que os funcionários estejam cientes de suas responsabilidades de não armazenar nem copiar dados do portador do cartão para o computador pessoal local ou outras mídias, sua empresa deve contar com uma política que proíba claramente essas atividades.</p>

Requisito	Orientação
<p><b>12.4</b> Certificar-se de que a política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todos os funcionários e prestadores de serviços.</p>	<p>Sem papéis e responsabilidades claramente definidos e atribuídos, 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>12.5</b> Atribuir um indivíduo ou uma equipe às seguintes responsabilidades de gerenciamento da segurança das informações:</p> <ul style="list-style-type: none"> <li><b>12.5.1</b> Estabelecimento, documentação e distribuição de políticas e procedimentos de segurança</li> <li><b>12.5.2</b> Monitoramento e análise de alertas e informações de segurança, e distribuição para as equipes apropriadas</li> <li><b>12.5.3</b> Definição, documentação e distribuição dos procedimentos de resposta e escalção de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente</li> <li><b>12.5.4</b> Administração das contas dos usuários, incluindo adições, exclusões e modificações</li> <li><b>12.5.5</b> Monitoramento e controle de todo acesso aos dados</li> </ul>	<p>Cada pessoa ou equipe com responsabilidades pela gestão da segurança das informações 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 portador do cartão.</p>
<p><b>12.6</b> Implementar um programa formal de conscientização da segurança para conscientizar todos os funcionários sobre a importância da segurança dos dados do portador 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>12.6.1</b> Instruir os funcionários quando da contratação e pelo menos uma vez por ano.</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 portador do cartão.</p>
<p><b>12.6.2</b> Exigir que os funcionários reconheçam, pelo menos uma vez por ano, que leram e compreenderam a política e os procedimentos de segurança da empresa.</p>	<p>Exigir um reconhecimento por parte dos funcionários (por exemplo, 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>

Requisito	Orientação
<p><b>12.7</b> Selecionar funcionários potenciais (veja a definição de "funcionário" no item 9.2 acima) antes da contratação para minimizar o risco de ataques de fontes internas.</p> <p><i>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.</i></p>	<p>Executar investigações de histórico completas antes de contratar funcionários que se esperam ter acesso aos dados do portador do cartão reduz o risco do uso não autorizado de PANs e outros dados do portador do cartão por pessoas com históricos questionáveis ou criminais. Espera-se que uma empresa tenha uma política e um processo para verificações de histórico, incluindo o próprio processo de decisão para o qual os resultados da verificação do histórico tenham impacto sobre as decisões de contratação (e qual seria esse impacto).</p>
<p><b>12.8</b> Se os dados do portador do cartão forem compartilhados com prestadores de serviços, manter e implementar políticas e procedimentos para gerenciar os prestadores de serviços, incluindo o seguinte:</p>	<p>Se o comerciante ou o prestador de serviço compartilhar os dados do portador 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><b>12.8.1</b> Manter uma lista dos prestadores de serviços.</p>	<p>Saber quem são os prestadores de serviço identifica quando possíveis riscos se estenderem para fora da organização.</p>
<p><b>12.8.2</b> Manter um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do portador do cartão que eles possuem.</p>	<p>O reconhecimento dos prestadores de serviço evidencia o compromisso deles com manter uma segurança adequada dos dados do portador do cartão que são obtidos dos clientes e, assim, responsabiliza-os.</p>
<p><b>12.8.3</b> Deve haver um processo definido para a contratação dos prestadores de serviços, incluindo uma due diligence adequada antes da contratação.</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><b>12.8.4</b> Manter um programa para monitorar o status de conformidade quanto ao PCI DSS dos prestadores de serviços.</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.</p>
<p><b>12.9</b> Implementar um plano de resposta a incidentes. Preparar-se para reagir imediatamente a uma falha no sistema.</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>

Requisito	Orientação
<p><b>12.9.1</b> Criar o plano de resposta a incidentes a ser implementado no caso de falha no sistema. Certificar-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 back-up 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 de pagamento</li> </ul>	<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 portador do cartão.</p>
<p><b>12.9.2</b> Testar o plano pelo menos uma vez por ano.</p>	<p>Sem testes adequados, etapas essenciais podem ser perdidas, o que poderia limitar a exposição durante um incidente.</p>
<p><b>12.9.3</b> Designar equipes específicas para estarem disponíveis em tempo integral para reagir aos alertas.</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. Se não estiverem disponíveis recursos internos, pense em contratar um fornecedor que os forneça.</p>
<p><b>12.9.4</b> Fornecer o treinamento adequado à equipe que é responsável pela resposta às falhas do sistema.</p>	
<p><b>12.9.5</b> Incluir alertas de sistemas de detecção de invasão, prevenção contra invasões e monitoramento da integridade dos arquivos.</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>12.9.6</b> Desenvolver 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>

## Orientação para o Requisito A.1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada

### **Requisito A.1: Os provedores de hospedagem compartilhada devem proteger o ambiente de dados do portador do cartão**

Conforme mencionado no Requisito 12.8, todos os prestadores de serviços com acesso aos dados do portador do cartão (incluindo os provedores de hospedagem compartilhada) devem seguir o PCI DSS. Além disso, o Requisito 2.4 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 Anexo.

Requisito	Orientação
<p><b>A.1</b> Proteja o ambiente hospedado e os dados de cada entidade (seja comerciante, prestador de serviços ou outra entidade), de acordo com os itens A.1.1 a A.1.4: Um provedor de hospedagem deve atender a esses requisitos, assim como a todas as outras seções relevantes do PCI DSS.</p> <p><i>Observação: Embora um provedor de hospedagem possa atender a esses requisitos, a conformidade da entidade de que utiliza o provedor de hospedagem não é assegurada. Cada entidade deve estar em conformidade com o PCI DSS e validar a conformidade, conforme aplicável.</i></p>	<p>O Anexo 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. Essas etapas devem ser cumpridas, além de todos os outros requisitos relevantes do PCI DSS.</p>
<p><b>A.1.1</b> Certificar-se de que cada entidade executa somente os processos que têm acesso aos dados do portador do cartão daquela entidade.</p>	<p>Se um comerciante ou prestador de serviço puder executar seus aplicativos próprios no servidor compartilhado, eles devem ser executados com o ID de usuário do comerciante ou prestador de serviço, e não como um usuário privilegiado. O usuário privilegiado pode ter acesso aos ambientes de dados do portador do cartão de todos os outros comerciantes e prestadores de serviço, além dos seus próprios.</p>
<p><b>A.1.2</b> Restringir o acesso e os privilégios de cada entidade somente ao próprio ambiente de dados do portador do cartão.</p>	<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 do portador do cartão, considere o seguinte: (1) privilégios do ID de usuário do servidor da Web do comerciante ou do prestador de serviço; (2) permissões concedidas para ler, gravar e executar arquivos; (3) permissões concedidas para gravar em binários do sistema; (4) permissões concedidas aos arquivos de log do comerciante e do prestador de serviço; e (5) controles para garantir que um comerciante ou prestador de serviço não possa monopolizar os recursos do sistema.</p>

Requisito	Orientação
<b>A.1.3</b> Certificar-se de que os registros e as trilhas de auditoria estão ativadas e são exclusivas para o ambiente de dados do portador do cartão de cada entidade, além de estarem em conformidade com o Requisito 10 do PCI DSS.	Os logs 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 portador do cartão.
<b>A.1.4</b> Ativar processos para providenciar uma investigação forense oportuna no caso de um comprometimento em qualquer comerciante ou prestador de serviços hospedado.	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.

## Anexo A: Padrão de segurança de dados do PCI: documentos relacionados

Os documentos a seguir foram criados para auxiliar comerciantes e prestadores de serviço a entenderem o Padrão de segurança de dados do PCI e as responsabilidades e requisitos de conformidade.

Documento	Público
<i>Requisitos dos Padrões de Segurança de Dados do PCI e Procedimentos de Avaliação da Segurança</i>	Todos os comerciantes e prestadores de serviço
<i>Navegando pelo PCI DSS: Entendendo o porquê dos requisitos</i>	Todos os comerciantes e prestadores de serviço
<i>Padrão de segurança de dados do PCI: Diretrizes e instruções do Questionário de auto-avaliação</i>	Todos os comerciantes e prestadores de serviço
<i>Padrão de segurança de dados do PCI: Questionário A de auto-avaliação e atestado</i>	Comerciantes <sup>10</sup>
<i>Padrão de segurança de dados do PCI: Questionário B de auto-avaliação e atestado</i>	Comerciantes <sup>10</sup>
<i>Padrão de segurança de dados do PCI: Questionário C de auto-avaliação e atestado</i>	Comerciantes <sup>10</sup>
<i>Padrão de segurança de dados do PCI: Questionário D de auto-avaliação e atestado</i>	Comerciantes <sup>10</sup> e todos os prestadores de serviço
<i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>	Todos os comerciantes e prestadores de serviço

<sup>10</sup> Para determinar o Questionário de auto-avaliação adequado, veja *Padrão de segurança de dados do PCI: Diretrizes e instruções do Questionário de auto-avaliação*, “Selecionando o SAQ e certificado que melhor se aplica à sua organização”.