



**Setor de cartões de pagamento (PCI)  
Padrão de segurança de dados  
Questionário de auto-avaliação D e  
Atestado de conformidade**

---

**Todos os outros comerciantes e prestadores de  
serviço qualificados pelo SAQ**

**Versão 1.2**

Outubro de 2008

## Alterações no documento

---

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

## Índice

---

<b>Alterações no documento .....</b>	<b>i</b>
<b>Padrão de segurança de dados do PCI: documentos relacionados.....</b>	<b>iii</b>
<b>Antes de você começar .....</b>	<b>iv</b>
<b>Preenchendo o questionário de auto-avaliação.....</b>	<b>iv</b>
<b>Conformidade do PCI DSS – Etapas de preenchimento .....</b>	<b>iv</b>
<b>Orientação para não aplicabilidade e exclusão de determinados requisitos específicos</b>	<b>v</b>
<b>Atestado de conformidade, SAQ D — Versão do comerciante.....</b>	<b>1</b>
<b>Atestado de conformidade, SAQ D — Versão do prestador de serviço.....</b>	<b>4</b>
<b>Questionário de auto-avaliação D.....</b>	<b>7</b>
<b>Construa e mantenha uma rede segura.....</b>	<b>7</b>
<i>Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados ..</i>	<i>7</i>
<i>Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.....</i>	<i>9</i>
<b>Proteger os dados do portador do cartão.....</b>	<b>11</b>
<i>Requisito 3: Proteger os dados armazenados do portador do cartão.....</i>	<i>11</i>
<i>Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas .....</i>	<i>13</i>
<b>Manter um programa de gerenciamento de vulnerabilidades .....</b>	<b>14</b>
<i>Requisito 5: Usar e atualizar regularmente o software ou programas antivírus .....</i>	<i>14</i>
<i>Requisito 6: Desenvolver e manter sistemas e aplicativos seguros.....</i>	<i>14</i>
<b>Implementar medidas de controle de acesso rigorosas.....</b>	<b>17</b>
<i>Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios.....</i>	<i>17</i>
<i>Requisito 8: Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador .....</i>	<i>17</i>
<i>Requisito 9: Restringir o acesso físico aos dados do portador do cartão.....</i>	<i>19</i>
<b>Monitorar e testar as redes regularmente.....</b>	<b>21</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>21</i>
<i>Requisito 11: Testar regularmente os sistemas e processos de segurança .....</i>	<i>22</i>
<b>Manter uma política de segurança de informações .....</b>	<b>24</b>
<i>Requisito 12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços .....</i>	<i>24</i>
<b>Anexo A: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada.....</b>	<b>27</b>
<i>Requisito A.1: Os provedores de hospedagem compartilhada devem proteger o ambiente de dados do portador do cartão .....</i>	<i>27</i>
<b>Anexo B: Controles de compensação.....</b>	<b>28</b>
<b>Anexo C: Planilha dos controles de compensação.....</b>	<b>29</b>
<b>Planilha dos controles de compensação – Exemplo completo.....</b>	<b>30</b>
<b>Anexo D: Explicação de não aplicabilidade .....</b>	<b>31</b>

---

## 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 o SAQ do PCI DSS.

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 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>1</sup>
<i>Padrão de segurança de dados do PCI: Questionário B de auto-avaliação e atestado</i>	Comerciantes <sup>1</sup>
<i>Padrão de segurança de dados do PCI: Questionário C de auto-avaliação e atestado</i>	Comerciantes <sup>1</sup>
<i>Padrão de segurança de dados do PCI: Questionário D de auto-avaliação e atestado</i>	Comerciantes <sup>1</sup> e todos os prestadores de serviço
<i>Glossário de termos, abreviações e acrônimos do Padrão de segurança de dados do PCI e do Padrão de segurança de dados de aplicativos de pagamento</i>	Todos os comerciantes e prestadores de serviço

<sup>1</sup> Para determinar o Questionário de auto-avaliação adequado, veja *Padrão de segurança de dados do PCI: Diretrizes e instruções de auto-avaliação*, "Selecionando o SAQ e certificado que melhor se aplica à sua organização".

## Antes de você começar

### Preenchendo o questionário de auto-avaliação

O SAQ D foi desenvolvido para todos os prestadores de serviço qualificados pelo SAQ e para todos os comerciantes que não se encaixem nas descrições dos SAQs A-C, conforme descrito brevemente na tabela abaixo e integralmente em *Diretrizes e instruções do Questionário de auto-avaliação do PCI DSS*.

Tipo de validação do SAQ	Descrição	SAQ
1	Comerciantes do tipo cartão não presente (comércio eletrônico ou pedidos por correio/telefone), todas as funções dos dados do portador do cartão são terceirizadas. <i>Isso nunca se aplica a comerciantes presenciais.</i>	A
2	Comerciantes com máquinas de carbono, sem retenção eletrônica dos dados do portador do cartão	B
3	Comerciantes de terminal de discagem independente, sem retenção eletrônica dos dados do portador do cartão	B
4	Comerciantes com sistemas do POS conectados à Internet, sem retenção eletrônica dos dados do portador do cartão	C
5	Todos os outros comerciantes (não incluídos nas descrições dos SAQs A-C acima) e <b>todos</b> os prestadores de serviço definidos por uma bandeira como qualificados para preencherem um SAQ.	D

Os comerciantes que não se adequarem aos critérios dos SAQs A-C acima e todos os prestadores de serviço definidos por uma bandeira como qualificados pelo SAQ serão definidos como Tipo de Validação 5 do SAQ, aqui e em *Diretrizes e instruções do Questionário de auto-avaliação do PCI DSS*.

Apesar de várias organizações que preenchem o SAQ D precisarem validar a conformidade com todos os requisitos do PCI DSS, algumas organizações com modelos de negócio bastante específicos podem descobrir que alguns requisitos não se aplicam. Por exemplo: não se espera que uma empresa que não usa tecnologia wireless de forma alguma valide a conformidade com as seções do PCI DSS que são específicas da tecnologia wireless. Veja a orientação abaixo para obter informações sobre a exclusão da tecnologia wireless e determinados outros requisitos específicos.

Cada seção deste questionário se concentra em uma área específica de segurança, com base nas exigências do Padrão de segurança de dados do PCI.

### Conformidade do PCI DSS – Etapas de preenchimento

1. Preencha o Questionário de auto-avaliação (SAQ D) segundo as instruções do arquivo *Diretrizes e instruções do Questionário de auto-avaliação do PCI DSS*.
2. Faça uma varredura de vulnerabilidade aprovada com um Fornecedor Aprovado de Varredura (ASV) do PCI SSC e consiga provas de uma varredura aprovada dele.
3. Preencha integralmente o Atestado de conformidade.
4. Envie o SAQ, a comprovação de uma varredura aprovada e o Atestado de conformidade, junto com qualquer outra documentação solicitada, ao adquirente (para comerciantes) ou à bandeira de pagamento ou outro solicitante (para prestadores de serviços).

## Orientação para não aplicabilidade e exclusão de determinados requisitos específicos

**Exclusão:** Se você precisar responder o SAQ D para validar sua conformidade com o PCI DSS, as seguintes exceções podem ser consideradas. Veja abaixo “Não aplicabilidade” para obter uma resposta adequada do SAQ.

- As perguntas específicas ao wireless só precisarão ser respondidas se estiverem presentes em algum lugar da sua rede (por exemplo, Requisitos 1.2.3, 2.1.1 e 4.1.1). Observe que o Requisito 11.1 (uso do analisador wireless) ainda deverá ser respondido, mesmo se sua rede não tiver wireless, pois o analisador detecta intrusos ou dispositivos não autorizados que possam ter sido adicionados sem o conhecimento do comerciante.
- As questões específicas dos aplicativos e códigos personalizados (Requisitos 6.3-6.5) só precisarão ser respondidas se sua organização escrever os aplicativos da Web próprios.
- As perguntas dos Requisitos 9.1-9.4 só precisarão ser respondidas para instalações com “áreas confidenciais”, conforme definidas aqui. “Áreas confidenciais” referem-se a qualquer data center, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam 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.

**Não aplicabilidade:** Estes e outros requisitos considerados não aplicáveis ao seu ambiente deverão ser indicados com “N/A” na coluna “Especial” do SAQ. Da mesma forma, preencha a planilha “Explicação de não aplicabilidade”, no Anexo, para cada entrada “N/A”.

## Atestado de conformidade, SAQ D — Versão do comerciante

### Instruções para envio

O comerciante deve preencher este Atestado de conformidade como uma declaração do status de conformidade dele com os *Requisitos dos Padrões de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) e Procedimentos de Avaliação da Segurança*. Preencha todas as seções aplicáveis e consulte as instruções de envio em Conformidade do PCI DSS – Etapas de preenchimento, neste documento.

### Parte 1. Informações sobre a empresa do responsável pela avaliação da segurança qualificado (se aplicável)

Nome da empresa:				
Nome do PA-QSA líder:		Forma de tratamento:		
Telefone:		E-mail:		
Endereço comercial:		Cidade:		
Estado/Província:		País:	CEP:	
URL:				

### Parte 2. Informações sobre a organização do comerciante

Nome da empresa:		DBA(s):		
Contato:		Forma de tratamento:		
Telefone:		E-mail:		
Endereço comercial:		Cidade:		
Estado/Província:		País:	CEP:	
URL:				

### Parte 2a. Tipo de negócio do comerciante (assinale todas as alternativas que se aplicam):

- Varejista
  Telecomunicações
  Gêneros alimentícios e Supermercados  
 Petróleo
  E-Commerce
  Pedidos por correspondência/telefone  
 Outros (especificar):

Listar as áreas e locais incluídos na análise do PCI DSS:

### Parte 2b. Relações

Sua empresa se relaciona com um ou mais prestadores de serviços de terceiros (por exemplo, gateways, empresas de hospedagem na Web, agentes de passagens aéreas, agentes de programas de fidelidade, etc.)?  Sim  Não

Sua empresa se relaciona com mais de um adquirente?  Sim  Não

### Parte 2c. Processamento das transações

Aplicativo de pagamento sendo usado:	Versão do aplicativo de pagamento:
--------------------------------------	------------------------------------

### Parte 3. Validação do PCI DSS

Com base nos resultados observados no SAQ D datado de (*data de preenchimento*), o estabelecimento (*nome da empresa do comerciante*) confirma o seguinte estado de conformidade (marque uma opção):

**Em conformidade:** Todas as seções do PCI SAQ estão preenchidas, todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **CONFORME**; e uma varredura de verificação foi preenchida por um Fornecedor Aprovado de Varredura do PCI SSC, de forma que o estabelecimento (*nome da empresa do comerciante*) demonstrou conformidade total com o PCI DSS.

**Não conforme:** Nem todas as seções do PCI DSS SAQ estão preenchidas, ou nem todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **NÃO CONFORME**; ou uma varredura de verificação foi preenchida por um Fornecedor Aprovado de Varredura do PCI SSC, de forma que o estabelecimento (*nome da empresa do comerciante*) não demonstrou conformidade total com o PCI DSS.

**Data prevista** quanto à conformidade:

Uma entidade que estiver enviando esse formulário com um status de Não Conformidade talvez tenha de preencher o Plano de Ação na Parte 4 desse documento. *Verifique com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

### Parte 3a. Confirmação do status em conformidade

**O comerciante confirma que:**

- O Questionário de auto-avaliação D do PCI DSS, Versão (*versão do SAQ*), foi preenchido segundo as instruções nele contidas.
- Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação em todos os aspectos materiais.
- Eu confirmei com meu fornecedor do aplicativo de pagamento o aplicativo não armazena dados de autenticação confidenciais após a autorização.
- Eu li o PCI DSS e reconheço que sempre devo manter a total conformidade total com o PCI DSS.
- Não há evidências de armazenamento de dados<sup>2</sup> da tarja magnética (ou seja, rastro), dados<sup>3</sup> de CAV2, CVC2, CID ou CVV2, ou dados<sup>4</sup> de PIN depois que a autorização da transação foi localizada em QUAISQUER sistemas analisados durante essa avaliação.

### Parte 3b. Confirmação do comerciante

<i>Assinatura do responsável executivo pelo comerciante</i> ↑	<i>Data</i> ↑
<i>Nome do responsável executivo pelo comerciante</i> ↑	<i>Forma de tratamento</i> ↑

*Empresa do comerciante representada* ↑

<sup>2</sup> Dados codificados na fita magnética utilizados para autorização durante a transação com o cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados de rastro que podem ser retidos são o número da conta, a data de vencimento e o nome.

<sup>3</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>4</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.

#### Parte 4. Plano de ação referente ao status de não conformidade

Selecione o "Status de conformidade" adequado para cada requisito. Se você responder "NÃO" a qualquer um dos requisitos, será solicitado que a data na qual a empresa estará em conformidade seja fornecida além do requisito e de uma descrição resumida das ações que estão sendo realizadas para atender ao requisito. *Verifique com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Requisito do PCI DSS	Descrição do requisito	Status de conformidade (Selecione um)		Data e ações para solucionar (se o Status de conformidade for "NÃO")
		SIM	NÃO	
1	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteger os dados armazenados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas	<input type="checkbox"/>	<input type="checkbox"/>	
5	Usar e atualizar regularmente o software antivírus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desenvolver e manter sistemas e aplicativos seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios	<input type="checkbox"/>	<input type="checkbox"/>	
8	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir o acesso físico aos dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
11	Testar regularmente os sistemas e processos de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
12	Manter uma política que aborde a segurança das informações	<input type="checkbox"/>	<input type="checkbox"/>	

## Atestado de conformidade, SAQ D — Versão do prestador de serviço

### Instruções para envio

O prestador de serviço deve preencher este Atestado de conformidade como uma declaração do status de conformidade dele com os *Requisitos dos Padrões de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) e Procedimentos de Avaliação da Segurança*. Preencha todas as seções aplicáveis e consulte as instruções de envio em Conformidade do PCI DSS – Etapas de preenchimento, neste documento.

#### Parte 1. Informações sobre a empresa do responsável pela avaliação da segurança qualificado (se aplicável)

Nome da empresa:			
Nome do PA-QSA líder:	Forma de tratamento:		
Telefone:	E-mail:		
Endereço comercial:	Cidade:		
Estado/Província:	País:	CEP:	
URL:			

#### Parte 2. Informações sobre a organização do prestador de serviços

Nome da empresa:			
Contato:	Forma de tratamento:		
Telefone:	E-mail:		
Endereço comercial:	Cidade:		
Estado/Província:	País:	CEP:	
URL:			

#### Parte 2a. Serviços

##### Serviços fornecidos (assinale todos os que se aplicam):

- |                                                |                                                    |                                                                   |
|------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------|
| <input type="checkbox"/> Autorização           | <input type="checkbox"/> Programas de fidelidade   | <input type="checkbox"/> Servidor de Controle de Acesso Seguro 3D |
| <input type="checkbox"/> Comutação             | <input type="checkbox"/> IPSP (E-commerce)         | <input type="checkbox"/> Processar transações com tarja magnética |
| <input type="checkbox"/> Gateway de pagamentos | <input type="checkbox"/> Compensação e liquidação  | <input type="checkbox"/> Processar transações MO/TO               |
| <input type="checkbox"/> Hospedagem            | <input type="checkbox"/> Processamento de emissões | <input type="checkbox"/> Outros (especificar):                    |

Listar as áreas e locais incluídos na análise do PCI DSS:

#### Parte 2b. Relações

Sua empresa se relaciona com um ou mais prestadores de serviços de terceiros (por exemplo, gateways, empresas de hospedagem na Web, agentes de passagens aéreas, agentes de programas de fidelidade, etc.)?  Sim  Não

#### Parte 2c: Processamento das transações

Como e em qual capacidade seu negócio armazena, processa e/ou transmite dados do portador do cartão?

Aplicativos de pagamento em uso ou fornecidos como parte de seu serviço:	Versão do aplicativo de pagamento:
--------------------------------------------------------------------------	------------------------------------

### Parte 3. Validação do PCI DSS

Com base nos resultados observados no SAQ D datado de (*data de preenchimento do SAQ*), o estabelecimento (*nome da empresa do prestador de serviços*) confirma o seguinte estado de conformidade (marque uma opção):

- Em conformidade:** Todas as seções do PCI SAQ estão preenchidas, todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **CONFORME**; e uma varredura de verificação foi preenchida por um Fornecedor Aprovado de Varredura do PCI SSC, de forma que (*nome da empresa do prestador de serviços*) demonstrou conformidade total com o PCI DSS.
- Não conforme:** Nem todas as seções do PCI SAQ estão preenchidas, ou algumas todas as perguntas foram respondidas negativamente, resultando em uma classificação geral de **NÃO CONFORME**; ou uma varredura de verificação foi preenchida por um Fornecedor Aprovado de Varredura do PCI SSC, de forma que o estabelecimento (*nome da empresa do prestador de serviços*) não demonstrou conformidade total com o PCI DSS.

**Data prevista** quanto à conformidade:

Uma entidade que estiver enviando esse formulário com um status de Não Conformidade talvez tenha de preencher o Plano de Ação na Parte 4 desse documento. Verifique com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.

### Parte 3a. Confirmação do status em conformidade

**Prestador de serviço confirma:**

- O Questionário de auto-avaliação D, Versão (*insira o número da versão*), foi preenchido segundo as instruções nele contidas.
- Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação.
- Eu li o PCI DSS e reconheço que sempre devo manter a total conformidade total com o PCI DSS.
- Não há evidências de armazenamento de dados<sup>5</sup> da tarja magnética (ou seja, rastro), dados<sup>6</sup> de CAV2, CVC2, CID ou CVV2, ou dados<sup>7</sup> de PIN depois que a autorização da transação foi localizada em QUAISQUER sistemas analisados durante essa avaliação.

### Parte 3b. Confirmação do prestador de serviço

<i>Assinatura do responsável executivo pelo prestador de serviços</i> ↑	<i>Data</i> ↑
<i>Nome do responsável executivo pelo prestador de serviços</i> ↑	<i>Forma de tratamento</i> ↑

*Representante da empresa prestadora de serviços* ↑

<sup>5</sup> Dados codificados na fita magnética utilizados para autorização durante a transação com o cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados de rastro que podem ser retidos são o número da conta, a data de vencimento e o nome.

<sup>6</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>7</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.

#### Parte 4. Plano de ação referente ao status de não conformidade

Selecione o "Status de conformidade" adequado para cada requisito. Se você responder "NÃO" a qualquer um dos requisitos, será solicitado que a data na qual a empresa estará em conformidade seja fornecida além do requisito e de uma descrição resumida das ações que estão sendo realizadas para atender ao requisito. *Verifique com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Requisito do PCI DSS	Descrição do requisito	Status de conformidade (Selecione um)		Data e ações para solucionar (se o Status de conformidade for "NÃO")
		SIM	NÃO	
1	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteger os dados armazenados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas	<input type="checkbox"/>	<input type="checkbox"/>	
5	Usar e atualizar regularmente o software antivírus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desenvolver e manter sistemas e aplicativos seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios	<input type="checkbox"/>	<input type="checkbox"/>	
8	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir o acesso físico aos dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
11	Testar regularmente os sistemas e processos de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
12	Manter uma política que aborde a segurança das informações	<input type="checkbox"/>	<input type="checkbox"/>	

## Questionário de auto-avaliação D

Data de preenchimento:

### Construa e mantenha uma rede segura

#### Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
1.1	Os padrões estabelecidos de configuração de firewall e roteador incluem o seguinte?				
1.1.1	Processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	Diagramas da rede atual com todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes wireless?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	Requisitos para um firewall em cada conexão da Internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Descrição de grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	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?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Requisito para analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2	A configuração do firewall restringe as conexões entre redes não confiáveis e qualquer sistema no ambiente de dados do portador do cartão, da seguinte forma: <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>				
1.2.1.	Restringir o tráfego de entrada e saída para aquele que é necessário para o ambiente de dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.2	Proteger e sincronizar os arquivos de configuração do roteador?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Incluir a instalação de firewalls de perímetro entre quaisquer redes wireless e o ambiente de dados do portador do cartão, e configurar esses firewalls para recusar ou controlar (se esse tráfego for necessário para fins comerciais) qualquer tráfego a partir do ambiente wireless no ambiente de dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Não aplicável" (N/A) ou "Controle de compensação utilizado". As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
1.3	O firewall proíbe o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do portador do cartão?				
1.3.1	Está implementada 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?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	O tráfego de Internet de entrada está limitado a endereço de IP dentro da DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	Os roteamentos diretos estão proibidos para tráfego de entrada ou saída entre a Internet e o ambiente dos dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	Os endereços internos estão proibidos de serem passados da internet para a DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Está restringido o tráfego de saída do ambiente de dados do portador do cartão à Internet de uma forma que o tráfego de saída possa acessar somente endereços IP na DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	A inspeção com status, também conhecida como filtragem de pacote dinâmico, está implementada (ou seja, somente conexões estabelecidas podem entrar na rede)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	O banco de dados está posicionado em uma zona da rede interna, separada da DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	Foi implementado o mascaramento de IP para impedir que endereços internos sejam traduzidos e revelados na Internet, usando o espaço de endereço RFC 1918? <i>Usar as tecnologias NAT (network address translation)—por exemplo, PAT (port address translation).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
1.4	Foi instalado 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 são usados para acessar a rede da empresa?		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

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

Pergunta		Resposta:	Sim	Não	Especial*
2.1	Os valores-padrão entregues pelo fornecedor são sempre alterados <b>antes</b> de instalar um sistema na rede? <i>Os exemplos incluem senhas, SNMP (simple network management protocol) strings da comunidade e eliminação de contas desnecessárias.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	(a) Os padrões** dos ambientes wireless conectados ao ambiente dos dados do portador do cartão ou a transmissão dos dados do portador do cartão são alterados antes de instalar um sistema wireless? <i>** Os padrões desse ambiente wireless incluem, mas não de forma exclusiva, chaves-padrão de criptografia wireless, senhas e strings da comunidade SNMP.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) As configurações de segurança do dispositivo wireless estejam ativadas com relação a uma tecnologia de criptografia robusta para a autenticação e a transmissão?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Os padrões de configuração foram desenvolvidos para todos os componentes do sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Esses padrões resolvem todas as vulnerabilidade de segurança conhecidas e são coerentes com os padrões fortalecidos do sistema aceito pelo setor, como SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) e Center for Internet Security (CIS)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Os controles incluem o seguinte?				
2.2.1	Somente uma função principal é implementada por servidor?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Todos os serviços e protocolos desnecessários e inseguros (os serviços e protocolos que não precisam desempenhar diretamente a função especificada do dispositivo) foram desativados?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Os parâmetros de segurança do sistema estão configurados para evitar uso incorreto?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários foram removidas?		<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Todos os acessos administrativos não-console estão criptografados? <i>Usar tecnologias como SSH, VPN ou SSL/TLS para o gerenciamento baseado na Web e outros acessos administrativos não-console.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

	<b>Pergunta</b>	<b>Resposta:</b>	<b><u>Sim</u></b>	<b><u>Não</u></b>	<b><u>Especial*</u></b>
2.4	<p>Se você for um provedor de hospedagem compartilhada, os sistemas estão configurados para proteger o ambiente de hospedagem e os dados do portador do cartão?</p> <p><i>Veja o Anexo A: Outros Requisitos do PCI DSS para provedores de hospedagem compartilhados para requisitos específicos devem ser cumpridos.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	

## Proteger os dados do portador do cartão

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

	Pergunta	Resposta:	Sim	Não	Especial*
3.1	(a) O armazenamento dos dados do portador do cartão é mantido em um mínimo, e a quantidade de armazenamento e o tempo de retenção estão limitados àquilo que é exigido para fins corporativos, jurídicos e/ou regulatórios?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Existe uma política de retenção e descarte de dados? E ela inclui as limitações definidas no item (a) acima?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Todos os sistemas cumprem os seguintes requisitos em relação ao armazenamento de dados de autenticação confidenciais após a autorização (mesmo se criptografados)?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>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. NUNCA armazene códigos ou valores de verificação do cartão ou elementos de dados de valor de verificação do PIN.</i></p> <p><i>Observação: Veja Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter mais informações.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>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>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Não armazenar o PIN ( <i>personal identification number</i> ) ou o bloco de PIN criptografado.		<input type="checkbox"/>	<input type="checkbox"/>	
3.3	<p>O PAN é mascarado 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>Este requisito não se aplica aos funcionários e outras partes interessadas que precisam visualizar o PAN completo.</i></li> <li>▪ <i>Este 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.</i></li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
3.4	<p>O PAN é, no mínimo, ilegível em qualquer local onde ele esteja armazenado em mídia digital portátil, mídia de back-up, em registros) utilizando qualquer uma das seguintes abordagens?</p> <ul style="list-style-type: none"> <li>▪ Hashing de direção única com base na criptografia robusta</li> <li>▪ Truncamento</li> <li>▪ Tokens de índice e pads (os pads devem ser armazenados de forma segura)</li> <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>Se, por algum motivo, uma empresa não puder tornar o PAN ilegível, consulte o Anexo B: "Controles de compensação".</i></p> <p><i>Observação: "Criptografia robusta" é definida em Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	<p>Se a criptografia de disco (e não a criptografia do banco de dados no nível de coluna ou de arquivo) for utilizada:</p> <p>(a) O acesso lógico é gerenciado de forma independente dos mecanismos de controle de acesso ao sistema operacional (por exemplo, não usando bancos de dados de conta de usuário local)?</p> <p>(b) As chaves de descompactação independem das contas do usuário?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	As chaves criptográficas usadas para a criptografia dos dados do portador do cartão estão protegidas contra a divulgação e o uso incorreto?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	O acesso às chaves criptográficas está restrito ao menor número necessário de responsáveis pela proteção?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	As chaves criptográficas são armazenadas com segurança e no menor número possível de locais e formas?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6	<p>(a) Todos os principais processos e procedimentos de gerenciamento para as chaves criptográficas são usados para criptografar os dados do portador do cartão, totalmente documentados e implementados?</p> <p>(b) Eles incluem o seguinte?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.1	Geração de chaves criptográficas robustas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Distribuição segura de chaves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Armazenamento seguro de chaves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	<p>Troca periódica das 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>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Inutilização ou substituição de chaves criptográficas comprometidas antigas ou suspeitas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Compartilhamento do conhecimento e a determinação do controle duplo de chaves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
3.6.7	Prevenção contra a substituição não autorizada de chaves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Requisito para que os responsáveis pela proteção das chaves criptográficas assinem um formulário declarando que eles compreendem e aceitam suas responsabilidades de responsáveis pela proteção das chaves		<input type="checkbox"/>	<input type="checkbox"/>	

**Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas**

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
4.1	São utilizadas 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? <i>Exemplos de redes públicas, abertas, que se encontram no escopo do PCI DSS são a Internet, tecnologias wireless, GSM (Global System for Mobile) e GPRS (General Packet Radio Service).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	As melhores práticas do setor (por exemplo, IEEE 802.11i) são usadas para implementar a criptografia robusta para a autenticação e a transmissão e para a transmissão de dados do portador do cartão ou estejam conectadas ao ambiente de dados do portador do cartão? <i>Observações:</i> <ul style="list-style-type: none"> <li>▪ <i>Para novas implementações wireless, será proibido implementar o WEP após 31 de março de 2009.</i></li> <li>▪ <i>Para as implementações wireless atuais, será proibido implementar o WEP após 30 de junho de 2010.</i></li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	
4.2	Estão implementados procedimentos, políticas e práticas para evitar o envio de PANs não criptografados por tecnologias de mensagem do usuário final (como e-mail, mensagens instantâneas, chat)?		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

## Manter um programa de gerenciamento de vulnerabilidades

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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
5.1	Os softwares antivírus estão implementados em todos os sistemas normalmente afetados por softwares mal-intencionados (especialmente em computadores pessoais e servidores)?		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Todos os programas antivírus podem detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados?		<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Todos os mecanismos antivírus estão atualizados, funcionando ativamente, e conseguem gerar logs de auditoria?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
6.1	(a) Todos os componentes do sistema e softwares têm os patches de segurança mais recentes disponibilizados pelos fornecedores instalados?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os patches de segurança críticos foram instalados até um mês após o lançamento? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) Existe um processo para identificar as vulnerabilidades de segurança descobertas recentemente (por exemplo, inscrever-se em serviços de alerta disponíveis gratuitamente na Internet)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os padrões de configuração estão atualizados conforme exigido pelo Requisito 2.2 do PCI DSS para solucionar novos problemas de vulnerabilidade?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Aplicativos de software estão desenvolvidos de acordo com o PCI DSS (por exemplo, autenticação segura e registros) e com base nas melhores práticas do setor, e eles incorporam a segurança das informações em todo o ciclo de vida do desenvolvimento dos softwares?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os controles incluem o seguinte?				
6.3.1	Teste de todos os patches de segurança e alterações de configuração no sistema e no software antes da implementação, incluindo, mas não se limitando a, o seguinte:		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.1	Validação de toda entrada (para impedir scripting de site cruzado, falhas na injeção, execução de arquivos maliciosos, etc.)		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
6.3.1.2	Validação de manuseio de erros adequado		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validação de armazenamento criptográfico seguro		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validação das comunicações seguras		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validação de controle de acesso adequado baseado na função (RBAC)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Ambientes de desenvolvimento/testes e de produção separados?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Remoção dos dados de teste e contas antes que os sistemas de produção tornem-se ativos?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.6	Remoção das contas dos aplicativos personalizados, IDs e senhas de usuários antes que os aplicativos tornem-se ativos ou sejam liberados para os clientes?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.7	Análise do código personalizado antes de liberar para produção ou para os clientes com o objetivo de identificar qualquer vulnerabilidade potencial de codificação? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) Os procedimentos de controle de alterações foram seguidos para todas as alterações nos componentes do sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os procedimentos garantem o seguinte?				
6.4.1	Documentação de impacto?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Endosso da gerência pelas partes apropriadas?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Teste da funcionalidade operacional?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Procedimentos de back-out?		<input type="checkbox"/>	<input type="checkbox"/>	

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
6.5	(a) Todos os aplicativos da Web (internos e externos, e incluindo o acesso administrativo na Web ao aplicativo) foram desenvolvidos com base nas diretrizes de codificação seguras, como o <i>Guia do projeto de segurança do aplicativo aberto da Web</i> ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) A prevenção de vulnerabilidades de codificação comuns está coberta nos processos de desenvolvimento do software, incluindo o seguinte? <i>Observação: As vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas no guia OWASP quando o PCI DSS v1.2 foi publicado. No entanto, se e quando o guia OWASP for atualizado, a versão atualizada deverá ser usada para essas exigências.</i>				
6.5.1	Scripting de site cruzado (XSS)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Falhas na injeção, particularmente na injeção SQL? <i>Considerar também as falhas de injeção LDAP e Xpath, assim como outras falhas.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Execução de arquivo mal-intencionado?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Referências diretas a objetos inseguros?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Falsificação de solicitações de site cruzado (CSRF)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Vazamento de informações e resolução incorreta de erros?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Autenticação quebrada e gerenciamento de sessão?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Armazenamento criptográfico seguro?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Comunicações inseguras?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Falha em restringir o acesso a URLs?		<input type="checkbox"/>	<input type="checkbox"/>	
6.6	Para aplicativos da Web voltados ao público, são abordadas novas ameaças e vulnerabilidades continuamente? E é assegurado que esses aplicativos estejam protegidos contra ataques conhecidos por <i>qualquer um</i> dos métodos a seguir? <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; ou</li> <li>▪ Instalar um firewall na camada de aplicativos da Web diante de aplicativos da Web voltados ao público</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

## 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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
7.1	(a) O acesso aos componentes do sistema e aos dados do portador do cartão somente àquelas pessoas cuja função requer tal acesso?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) As limitações de acesso incluem o seguinte:				
7.1.1	Restrição dos direitos de acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	A concessão dos privilégios está baseada na classificação e na atribuição da função da equipe individual?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	O requisito de um formulário de autorização assinado pela gerência que especifica os privilégios exigidos?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementação de um sistema de controle de acesso automático?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) Existe um controle de acesso para sistemas com vários usuários, a fim de restringir o acesso com base no conhecimento do usuário, e ele está configurado para “negar tudo”, a menos que especificamente permitido?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Esse sistema de controle de acesso inclui o seguinte:				
7.2.1	Cobertura de todos os componentes do sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	A concessão dos privilégios às pessoas está baseada na classificação e na atribuição da função?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Configuração padrão “recusar todos”?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
8.1	Todos os usuários recebem um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
8.2	Além de atribuir um ID exclusivo, um ou mais dos seguintes métodos foi empregado para autenticar todos os usuários? <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>		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:		
		Sim	Não	Especial*
8.3	A autenticação com dois fatores foi incorporada ao acesso remoto (acesso no nível da rede que se origina fora dela) à rede pelos funcionários, administradores e terceiros? <i>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.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
8.4	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> )?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Existe 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?			
8.5.1	O acréscimo, a exclusão e a modificação dos IDs do usuário, credenciais e outros objetos do responsável pela identificação são controlados?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	A identidade do usuário é verificada antes de executar redefinições de senha?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	As senhas iniciais são configuradas com um valor exclusivo para cada usuário, cabendo a cada um alterar sua senha imediatamente após o primeiro uso?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	O acesso a usuários desligados da empresa é imediatamente revogado?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	As contas inativas de usuários são removidas ou desativadas pelo menos a cada 90 dias?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	Existem contas usadas pelos fornecedores somente para a manutenção remota durante o período necessário?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Os procedimentos e políticas de senha são transmitidos a todos os usuários que têm acesso aos dados do portador do cartão?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	As contas e senhas de grupo, compartilhadas e genéricas são proibidas?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	As senhas de usuários devem ser alteradas pelo menos a cada 90 dias?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	É exigido um comprimento mínimo de senha de pelo menos sete caracteres?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	As senhas devem conter caracteres numéricos e alfabéticos?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	A pessoa deve enviar uma nova senha que seja diferente de qualquer uma das quatro últimas senhas utilizadas?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	Tentativas de acesso repetidas estão limitadas ao bloquear o ID do usuário após seis tentativas, no máximo?	<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
8.5.14	A duração do bloqueio está definida para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	Se uma sessão estiver ociosa por mais de 15 minutos, o usuário precisa redigitar a senha para reativar o terminal?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	O acesso a qualquer banco de dados contendo dados do portador do cartão é autenticado? (incluindo acesso por meio de aplicativos, administradores e todos os outros usuários).		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
9.1	São utilizados controles de entrada facilitados e adequados para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) São utilizados câmeras de vídeo ou outros mecanismos de controle de acesso para monitorar o acesso físico individual a áreas confidenciais? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) São coletados dados das câmeras vistas e correlacionadas a outras entradas?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Os dados das câmeras de vídeo são armazenados por pelo menos três meses, a menos que restrito por lei?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	O acesso físico a tomadas de rede acessíveis ao público é restrito?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	O acesso físico é restrito a pontos de acesso wireless, gateways e dispositivos portáteis?		<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Existem 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? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Todos os visitantes passam pelos procedimentos:				

\* "Não aplicável" (N/A) ou "Controle de compensação utilizado". As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
9.3.1	Autorizados antes de adentrar as áreas onde os dados do portador do cartão são processados ou mantidos?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.2	Um token físico é fornecido (por exemplo, um crachá ou dispositivo de acesso) que expira e que identifica os visitantes como não sendo funcionários?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	É solicitado que os visitantes apresentem o token físico antes de sair das dependências ou na data do vencimento?		<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) É utilizado um registro de visitantes para manter uma trilha de auditoria física da atividade do visitante?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) São registrados no log o nome do visitante, a empresa representada e o funcionário que autoriza o acesso físico?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Esse registro é mantido por pelo menos três meses, a menos que seja restringido de outra forma pela lei?		<input type="checkbox"/>	<input type="checkbox"/>	
9.5	(a) Back-ups de mídia são armazenados em um local seguro, de preferência em uma área externa, como um local alternativo ou de back-up, ou uma área de armazenamento comercial?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) A segurança do local é revisada pelo menos uma vez por ano?		<input type="checkbox"/>	<input type="checkbox"/>	
9.6	Todos os documentos impressos e as mídias eletrônicas que contêm dados do portador do cartão estão protegidos fisicamente?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia que contenha dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os controles incluem o seguinte:				
9.7.1	A mídia está classificada para que possa ser identificada como confidencial?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	A mídia foi enviada via mensageiro seguro ou outro método de entrega que possa ser monitorado com precisão?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Existem processos e procedimentos para garantir que a aprovação da gestão seja obtida antes de transferir toda e qualquer mídia contendo dados do portador do cartão de uma área protegida (especialmente quando a mídia for distribuída a pessoas físicas)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9	É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias que contêm dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	(a) Os logs de inventário de toda a mídia recebe manutenção adequada?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Os inventários de mídia são conduzidos pelo menos anualmente?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10	A mídia que contém os dados do portador do cartão é destruída quando ela não é mais necessária por razões corporativas ou legais? A destruição deve ser da seguinte forma:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Os materiais impressos são fragmentados, incinerados ou reciclados, de forma que os dados do portador do cartão não possam ser reconstruídos?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	A mídia eletrônica com os dados do portador do cartão ficam irrecuperáveis, de forma que os dados do portador do cartão não possam ser reconstruídos?		<input type="checkbox"/>	<input type="checkbox"/>	

## 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

Pergunta		Resposta:	Sim	Não	Especial*
10.1	Existe um processo para vincular todos os acessos aos componentes do sistema (principalmente o acesso realizado com privilégios administrativos como raiz) para cada usuário individual?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2	Foram implementadas trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:				
10.2.1	Todos os usuários têm acesso aos dados do portador do cartão?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.2	Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.3	Acesso a todas as trilhas de auditoria?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.4	Tentativas de acesso lógico inválidas?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.5	Uso de mecanismos de identificação e autenticação?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.6	Inicialização dos logs de auditoria?	<input type="checkbox"/>	<input type="checkbox"/>		
10.2.7	Criação e exclusão de objetos do nível do sistema?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3	As seguintes entradas da trilha de auditoria são registradas para todos os componentes do sistema para cada evento:				
10.3.1	Identificação do usuário?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3.2	Tipo de evento?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3.3	Data e hora?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3.4	Indicação de sucesso ou falha?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3.5	Origem do evento?	<input type="checkbox"/>	<input type="checkbox"/>		
10.3.6	A identidade ou o nome dos dados afetados, componentes do sistema ou recurso?	<input type="checkbox"/>	<input type="checkbox"/>		
10.4	Todos os relógios e horários do sistema crítico estão sincronizados?	<input type="checkbox"/>	<input type="checkbox"/>		
10.5	(a) As trilhas de auditoria são protegidas de forma que não possam ser alteradas?	<input type="checkbox"/>	<input type="checkbox"/>		
	(b) Os controles incluem o seguinte?				
10.5.1	A visualização da exibição de trilhas de auditoria está restrita às pessoas que têm uma necessidade relacionada à função?	<input type="checkbox"/>	<input type="checkbox"/>		
10.5.2	Os arquivos da trilha de auditoria são protegidos contra modificações não autorizadas?	<input type="checkbox"/>	<input type="checkbox"/>		
10.5.3	Os arquivos da trilha de auditoria são prontamente guardados em backup em um servidor de log centralizado ou mídia que seja difícil de alterar?	<input type="checkbox"/>	<input type="checkbox"/>		

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
10.5.4	Os registros quanto às tecnologias externas estão documentados em um servidor de registros na LAN interna?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos registros são usados 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
10.6	Os logs de todos os componentes do sistema são revisados pelo menos diariamente? <i>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). Observação: As ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6</i>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	O histórico da trilha de auditoria é mantido 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)?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pergunta		Respost	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
11.1	São feitos testes para 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?		<input type="checkbox"/>	<input type="checkbox"/>	
11.2	São executadas 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)? <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>		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
11.3	(a) São realizados 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Esses testes de penetração incluem o seguinte:				
11.3.1	Testes de penetração na camada de rede?		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Testes de penetração na camada do aplicativo?		<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) Sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão são usados para monitorar todo o tráfego no ambiente de dados do portador do cartão e alertar as equipes sobre comprometimentos suspeitos?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Todos os mecanismos de detecção e prevenção contra invasões são mantidos atualizados?		<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Existe um software de monitoramento de integridade do arquivo para alertar os funcionários quanto à modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo?; e		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) O software está configurado para executar comparações críticas do arquivo pelo menos semanalmente? <i>Observação: Para fins de monitoramento da integridade dos arquivos, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. 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>		<input type="checkbox"/>	<input type="checkbox"/>	

## Manter uma política de segurança de informações

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

Pergunta		Resposta:	Sim	Não	Especial*
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada? E ela cumpre com os itens a seguir?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Atende a todos os requisitos do PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	Inclui um processo anual que identifica ameaças e vulnerabilidades e que resulta em uma avaliação de risco formal?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Inclui uma análise pelo menos uma vez por ano e atualizações quando o ambiente é modificado?		<input type="checkbox"/>	<input type="checkbox"/>	
12.2	São desenvolvidos 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) 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) foram desenvolvidas para definir o uso adequado dessas tecnologias para todos os funcionários e prestadores de serviços?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Essas políticas de utilização exigem os itens a seguir?				
12.3.1	Aprovação explícita da gerência?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Autenticação para o uso da tecnologia?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Uma lista de todos esses dispositivos e equipes com acesso?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Identificação dos dispositivos com proprietário, informações de contato e finalidade?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Usos aceitáveis das tecnologias?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Locais de rede aceitáveis quanto às tecnologias?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.7	Lista dos produtos aprovados pela empresa?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Desconexão automática das sessões quanto às tecnologias de acesso remoto após um período específico de inatividade?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Ativação das tecnologias de acesso remoto para fornecedores somente quando for necessário por parte dos fornecedores, com uma desativação imediata após o uso?		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	Sim	Não	Especial*
12.3.10	Ao acessar os dados do portador do cartão por meio de tecnologias de acesso remoto, a política especifica a proibição de cópia, transferência e armazenamento dos dados do portador do cartão em discos rígidos locais e mídias eletrônicas removíveis?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	A política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todos os funcionários e prestadores de serviços?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	As seguintes responsabilidades do gerenciamento da segurança da informação estão atribuídas a uma pessoa ou equipe?				
12.5.1	Estabelecimento, documentação e distribuição de políticas e procedimentos de segurança?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2	Monitoramento e análise de alertas e informações de segurança e distribuição para as equipes apropriadas?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.3	Definição, documentação e distribuição dos procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.4	Administração das contas dos usuários, incluindo adições, exclusões e modificações?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5	Monitoramento e controle de todo acesso aos dados?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	Foi implementado um programa formal de conscientização da segurança para conscientizar todos os funcionários sobre a importância da segurança dos dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.1	Os funcionários são instruídos na contratação e depois pelo menos uma vez ao ano?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Os funcionários precisam reconhecer, pelo menos uma vez por ano, que leram e compreenderam a política e os procedimentos de segurança da empresa?		<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Funcionários potenciais (veja a definição de "funcionário" no item 9.2 acima) são selecionados antes da contratação para minimizar o risco de ataques de fontes internas? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Se os dados do portador do cartão forem compartilhados com provedores de serviço, existem políticas e procedimentos mantidos e implementados para gerenciar prestadores de serviço? E essas políticas e procedimentos incluem os itens a seguir?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	É mantida uma lista de prestadores de serviço.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	É mantido 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.		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Não aplicável" (N/A) ou "Controle de compensação utilizado". As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
12.8.3	Deve haver um processo definido para a contratação dos prestadores de serviços, incluindo uma <i>due diligence</i> adequada antes da contratação.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	É mantido um programa para monitorar o status de conformidade quanto ao PCI DSS dos prestadores de serviços.		<input type="checkbox"/>	<input type="checkbox"/>	
12.9	Foi implementado um plano de resposta a incidentes para incluir o seguinte, em preparação a reagir imediatamente a uma violação no sistema?				
12.9.1	(a) Foi criado um plano de resposta a incidentes para ser implementado em caso de violação do sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) O plano aborda, pelo menos:				
	▪ Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo a notificação às bandeiras de pagamento, pelo menos		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procedimentos de resposta específicos a incidentes		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procedimentos de recuperação e continuidade dos negócios		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Processos de back-up dos dados		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Análise dos requisitos legais visando ao relato dos comprometimentos		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Abrangência e resposta de todos os componentes críticos do sistema		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras de pagamento		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.2	O plano é testado pelo menos anualmente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	Equipes específicas são designadas para estarem disponíveis em tempo integral para reagir aos alertas?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	O treinamento adequado é prestado à equipe que é responsável pela resposta às falhas do sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	Estão incluídos alertas de sistemas de detecção de invasão, prevenção contra invasões e monitoramento da integridade dos arquivos?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	Existe 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?		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

## Anexo A: 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**

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
A.1	<p>O ambiente hospedado e os dados de cada entidade (seja comerciante, prestador de serviços ou outra entidade) estão protegidos de acordo com os itens A.1.1 a A.1.4:</p> <p><i>Um provedor de hospedagem deve atender a esses requisitos, assim como a todas as outras seções relevantes do PCI DSS.</i></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>				
A.1.1	Cada entidade executa processos que acessam somente o ambiente de dados do portador de cartão da entidade?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	Os acessos e privilégios de acesso de cada entidade restritos ao próprio ambiente dos dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	Os registros e as trilhas de auditoria estão ativados e são exclusivos para o ambiente de dados do portador do cartão de cada entidade, além de estarem em conformidade com o Requisito 10 do PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	Os processos estão ativados para providenciar uma investigação forense oportuna no caso de um comprometimento em qualquer comerciante ou prestador de serviços hospedado?		<input type="checkbox"/>	<input type="checkbox"/>	

\* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

## Anexo B: Controles de compensação

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

Os controles de compensação devem atender aos seguintes critérios:

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

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

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

- a) Os requisitos existentes do PCI DSS NÃO PODERÃO ser considerados como controles de compensação se já tiverem sido exigidos para o item sob análise. Por exemplo, as senhas para o acesso administrativo não console devem ser enviadas criptografadas para minimizar o risco de interceptação de senhas administrativas em texto simples. Uma entidade não pode usar outros requisitos de senha do PCI DSS (bloqueio contra invasores, senhas complexas, etc.) para compensar a falta de senhas criptografadas, já que esses outros requisitos de senha não minimizam o risco de interceptação de senhas em texto simples. Além disso, os outros controles de senha já são requisitos do PCI DSS referente ao item sob análise (contas).
  - b) Os requisitos existentes do PCI DSS PODERÃO ser considerados como controles de compensação se forem exigidos para outra área, mas não para o item sob análise. Por exemplo, uma autenticação com dois fatores é um requisito do PCI DSS para o acesso remoto. A autenticação com dois fatores *a partir da rede interna* também poderá ser considerada um controle de compensação para o acesso administrativo não console quando a transmissão de senhas criptografadas não for compatível. A autenticação com dois fatores poderá ser um controle de compensação aceitável se: (1) atender à intenção do requisito original ao abordar o risco de interceptação de senhas administrativas em texto simples; e (2) for configurada de modo adequado e em um ambiente seguro.
  - c) Os requisitos existentes do PCI DSS podem ser combinados com novos controles para se tornarem um controle de compensação. Por exemplo, se uma empresa não for capaz de tornar os dados do portador do cartão ilegíveis de acordo com o requisito 3.4 (por exemplo, por meio da criptografia), um controle de compensação poderia consistir de um dispositivo ou uma combinação de dispositivos, aplicativos e controles que abordam todos os itens a seguir: (1) segmentação da rede interna; (2) filtragem do endereço de IP ou endereço MAC; e (3) autenticação com dois fatores dentro da rede interna.
4. Ser proporcional ao risco adicional imposto pelo não cumprimento do requisito do PCI DSS.

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

## Anexo C: Planilha dos controles de compensação

Use esta planilha para definir os controles de compensação com relação a qualquer requisito no qual a opção "YES" (Sim) tenha sido assinalada e os controles de compensação tenham sido mencionados na coluna "Especial".

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

### Número e definição do requisito:

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

## Planilha dos controles de compensação – Exemplo completo

Use esta planilha para definir os controles de compensação com relação a qualquer requisito no qual a opção "YES" (Sim) tenha sido assinalada e os controles de compensação tenham sido mencionados na coluna "Especial".

**Número do requisito:** 8.1 — *Todos os usuários são identificados com um nome de usuário exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do portador do cartão?*

	Informações necessárias	Explicação
<b>1. Restrições</b>	Listar as restrições que impossibilitam a conformidade com o requisito original.	<i>A empresa XYZ utiliza Servidores Unix independentes sem LDAP. Sendo assim, cada um deles requer um login "raiz". A empresa XYZ não pode gerenciar o login "raiz" nem é possível registrar todas as atividades "raiz" por usuário.</i>
<b>2. Objetivo</b>	Definir o objetivo do controle original; identificar o objetivo atendido pelo controle de compensação.	<i>O objetivo de exigir logins exclusivos é duplo. Primeiro, não é considerado aceitável, da perspectiva de segurança, compartilhar credenciais de login. Segundo, ter logins compartilhados impossibilita afirmar em definitivo quem é responsável por uma determinada ação.</i>
<b>3. Risco identificado</b>	Identificar qualquer risco adicional imposto pela ausência do controle original.	<i>O risco adicional ocorre no sistema de controle de acesso ao não assegurar que todos os usuários tenham um ID exclusivo e possam ser monitorados.</i>
<b>4. Definição dos controles de compensação</b>	Definir os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	<i>A empresa XYZ solicitará que todos os usuários efetuem login nos servidores a partir dos seus desktops usando o comando SU. Esse comando permite que um usuário acesse a conta "raiz" e desempenhe ações na conta "raiz", mas possa efetuar login no diretório de registro do SU. Nesse caso, as ações de cada usuário podem ser monitoradas por meio da conta do SU.</i>
<b>5. Validação dos controles de compensação</b>	Definir como os controles de compensação foram validados e testados.	<i>A empresa XYZ demonstra ao responsável pela avaliação o comando SU que está sendo executado e se as pessoas que estão usando o comando efetuaram login para identificar que se o indivíduo está desempenhando ações com privilégios raiz.</i>
<b>6. Manutenção</b>	Definir o processo e os controles implementados para manter os controles de compensação.	<i>A empresa XYZ documenta os processos e procedimentos para assegurar que as configurações do SU não sejam modificadas, alteradas ou removidas para permitir que os usuários individuais executem comandos raiz sem serem monitorados ou efetuem login individualmente.</i>

