



**Indústria de cartões de pagamento (PCI)
Padrão de segurança de dados
Questionário de autoavaliação C
e Atestado de conformidade**

**Comerciantes com sistemas de
aplicativos de pagamento conectados à
internet – sem armazenamento eletrônico
dos dados do titular do cartão**

Para uso com o PCI DSS versão 3.2

Abril de 2016

Alterações no documento

Data	Versão do PCI DSS	Revisão de SAQ	Descrição
Outubro de 2008	1.2		Alinhar o conteúdo com o novo PCI DSS v1.2 e implementar alterações menores observadas desde a v1.1 original.
Outubro de 2010	2.0		Alinhar o conteúdo com os novos requisitos e procedimentos de teste do PCI DSS v2.0.
Fevereiro de 2014	3.0		Alinhar conteúdo com os requisitos do PCI DSS v3.0, testar procedimentos e incorporar opções de resposta adicional.
Abril de 2016	3.1		Atualizado para alinhar-se com a versão 3.1 do PCI DSS. Para detalhes das alterações do PCI DSS, consulte <i>PCI DSS – Resumo das Alterações de PCI DSS versão 3.0 para 3.1</i> .
Julho de 2015	3.1	1.1	Atualizado para remover as referências às "melhores práticas" antes de 30 de junho de 2015.
Abril de 2016	3.2	1.0	Atualizado para alinhar-se com o PCI DSS v 3.2. Para detalhes das mudanças de PCI DSS, consulte <i>PCI DSS – Resumo das Alterações de PCI DSS versão 3.1 para 3.2</i> .

Índice

Alterações no documento	i
Antes de você começar	iv
Etapas de conclusão da autoavaliação do PCI DSS.....	iv
Entendendo o Questionário de autoavaliação	v
<i>Teste esperado</i>	<i>v</i>
Preenchendo o questionário de autoavaliação.....	vi
Orientação para não aplicabilidade de determinados requisitos específicos.....	vi
Exceção legal	vi
Seção 1: Informações de avaliação	1
Seção 2: Questionário de autoavaliação C.....	4
Construir e manter a segurança de rede e sistemas.....	4
<i>Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados.....</i>	<i>4</i>
<i>Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança</i>	<i>6</i>
Proteger os dados do titular do cartão	12
<i>Requisito 3: Proteger os dados armazenados do titular do cartão.....</i>	<i>12</i>
<i>Requisito 4: Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas</i>	<i>14</i>
Manter um programa de gerenciamento de vulnerabilidades	16
<i>Requisito 5: Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus</i>	<i>16</i>
<i>Requisito 6: Desenvolver e manter sistemas e aplicativos seguros</i>	<i>18</i>
Implementar medidas rigorosas de controle de acesso	20
<i>Requisito 7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio</i>	<i>20</i>
<i>Requisito 8: Identificar e autenticar o acesso aos componentes do sistema</i>	<i>21</i>
<i>Requisito 9: Restringir o acesso físico aos dados do titular do cartão</i>	<i>24</i>
Monitorar e testar as redes regularmente.....	30
<i>Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão.....</i>	<i>30</i>
<i>Requisito 11: Testar regularmente os sistemas e processos de segurança</i>	<i>33</i>
Manter uma política de segurança de informações.....	39
<i>Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes</i>	<i>39</i>
Apêndice A: Requisitos adicionais do PCI DSS.....	43
<i>Anexo A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada.</i>	<i>43</i>
<i>Anexo A2: Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS.....</i>	<i>43</i>
<i>Apêndice A3: Validação Suplementar de Entidades Designadas (DESV).....</i>	<i>44</i>

Apêndice B: Planilha dos controles de compensação45

Apêndice C: Explicação de não aplicabilidade.....46

Seção 3: Detalhes de atestado e validação47

Antes de você começar

O SAQ C foi desenvolvido para abordar os requisitos aplicáveis aos comerciantes cujos sistemas de aplicativo de pagamento (como os sistemas de POS) estão conectados à internet (via conexão DSL, modem a cabo etc.).

Os comerciantes do SAQ C processam os dados do titular do cartão por meio de sistemas de POS ou outros sistemas de aplicativo de pagamento conectados à internet e não armazenam os dados do titular do cartão em nenhum sistema de computadores, podendo ser do tipo real (cartão presente) ou pedidos por correio/telefone (cartão não presente).

Os comerciantes SAQ C confirmam que, para esse canal de pagamento:

- Sua empresa possui um sistema de aplicativo de pagamento e uma conexão com a internet no mesmo dispositivo e/ou na mesma rede local (LAN);
- O sistema de aplicativo de pagamento/dispositivo de internet não está conectado a nenhum outro sistema no ambiente (isso pode ser feito por meio de segmentação da rede para isolar o sistema de aplicativo de pagamento/dispositivo de internet de todos os outros sistemas);
- O local físico do ambiente de POS não é conectado a outras instalações ou locais e qualquer LAN é somente para um local;
- Quaisquer dados do titular do cartão que sua empresa retém estão em papel (por exemplo, relatórios ou recibos impressos), e esses documentos não são recebidos eletronicamente; e
- Sua empresa não armazena dados do titular do cartão em formato eletrônico.

Esse SAQ não é aplicável para canais de Comércio eletrônico.

Esta versão reduzida do SAQ inclui perguntas que se aplicam a um tipo específico de ambiente de pequeno comerciante, conforme definido nos critérios de qualificação acima. Caso haja requisitos do PCI DSS aplicáveis ao seu ambiente que não estejam cobertos por este SAQ, pode ser um indício de que este SAQ não é adequado ao seu ambiente. Além disso, é necessário cumprir todos os requisitos aplicáveis do PCI DSS para estar em conformidade com o PCI DSS.

Etapas de conclusão da autoavaliação do PCI DSS

1. Identifique o SAQ aplicável para seu ambiente. Consulte o documento *Diretrizes e instruções do questionário de autoavaliação* no site da PCI SSC para obter informações.
2. Confirme que seu ambiente está adequadamente definido e atende aos critérios de elegibilidade para o SAQ que você está usando (como definido na Parte 2g do Atestado de conformidade).
3. Avalie seu ambiente quanto à conformidade com os requisitos de PCI DSS aplicáveis.
4. Conclua todas as seções desse documento:
 - Seção 1 (Partes 1 e 2 do AOC) – Informações de Avaliação e Sumário Executivo
 - Seção 2 – Questionário de autoavaliação do PCI DSS (SAQ C)
 - Seção 3 (Partes 3 e 4 do AOC) – Detalhes de validação e atestado e Plano de ação para requisitos que não estão em conformidade (se aplicável)
5. Envie o SAQ e Certificado de Conformidade (AOC), juntamente com qualquer outra documentação solicitada — como relatórios de varredura ASV — para seu adquirente, empresa de pagamento ou outro solicitante.

Entendendo o Questionário de autoavaliação

As perguntas contidas na coluna "Questão PCI DSS" deste questionário de autoavaliação são baseadas nos requisitos de PCI DSS.

Recursos adicionais que fornecem orientação sobre os requisitos de PCI DSS e como concluir o questionário de autoavaliação foram fornecidos para ajudar no processo de avaliação. Uma visão geral de alguns desses recursos é fornecida abaixo:

Documento	Inclui:
PCI DSS <i>(Requisitos dos padrões de segurança de dados do PCI e Procedimentos de avaliação da segurança)</i>	<ul style="list-style-type: none">• Orientação sobre o escopo• Orientação sobre a intenção de todos os requisitos de PCI DSS• Detalhes do teste de procedimentos• Orientação sobre os controles de compensação
Documentos de instruções e diretrizes do SAQ	<ul style="list-style-type: none">• Informações sobre todos os SAQs e seus critérios de elegibilidade• Como determinar qual SAQ é o correto para a sua organização
<i>Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS</i>	<ul style="list-style-type: none">• Descrições e definições de termos usados no PCI DSS e questionários de autoavaliação

Esses e outros recursos podem ser encontrados no site da PCI SSC (www.pcisecuritystandards.org). As organizações são encorajadas a revisar o PCI DSS e outros documentos de suporte antes de iniciar uma avaliação.

Teste esperado

As instruções fornecidas na coluna "Teste esperado" são baseadas nos procedimentos de teste no PCI DSS e fornecem uma descrição de alto nível dos tipos de atividades de teste que devem ser executadas para verificar se um requisito foi atendido. Os detalhes completos dos procedimentos de teste para todos os requisitos podem ser encontrados no PCI DSS.

Preenchendo o questionário de autoavaliação

Para cada questão, há uma escolha de respostas para indicar o status de sua empresa em relação ao requisito. **Somente uma resposta deve ser selecionada para cada questão.**

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

Resposta	Quando usar essa resposta:
Sim	O teste esperado foi executado e todos os elementos do requisito foram atendidos conforme consta.
Sim com CCW (Planilha de controles de compensação)	O teste esperado foi realizado e o requisito foi atendido com a ajuda de um controle de compensação. Todas as respostas nessa coluna exigem conclusão de uma Planilha de controles de compensação (CCW) no Apêndice B do SAQ. As informações sobre o uso dos controles de compensação e orientação sobre como preencher a planilha são fornecidas no PCI DSS.
Não	Alguns ou todos os elementos do requisito não foram atendidos, ou estão em processo para serem implementados, ou exigem mais testes antes de sabermos se estão de acordo.
N/D (Não disponível)	O requisito não é aplicável ao ambiente da organização (consulte a <i>Orientação para não aplicabilidade de determinados requisitos específicos</i> abaixo para ver exemplos). Todas as respostas nessa coluna exigem uma explicação de suporte no Apêndice C do SAQ.

Orientação para não aplicabilidade de determinados requisitos específicos

Apesar de várias organizações que preenchem o SAQ C precisarem validar a conformidade com todos os requisitos do PCI DSS nesse SAQ, 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 sem fio de forma alguma valide a conformidade com as seções do PCI DSS que são específicas da tecnologia sem fio (por exemplo, requisitos 1.2.3, 2.1.1 e 4.1.1). Observe que o Requisito 11.1 (uso de processos para identificar pontos de acesso sem fio não autorizados) deve ser respondido, mesmo que o dispositivo sem fio não esteja na sua rede, pois o processo detecta intrusos ou dispositivos não autorizados que possam ter sido adicionados sem seu conhecimento.

Se quaisquer requisitos forem considerados não aplicáveis ao seu ambiente, selecione a opção "N/D" para esse requisito específico e preencha a planilha "Explicação de não aplicabilidade" no Apêndice C para cada entrada "N/D".

Exceção legal

Se sua organização estiver sujeita a uma restrição legal que evite o cumprimento de um requisito de PCI DSS, marque a coluna "Não" para esse requisito e preencha o atestado relevante na Parte 3.

Seção 1: Informações de avaliação

Instruções para Envio

Esse documento deve ser preenchido como uma declaração do status de autoavaliação do comerciante com os *Requisitos do padrão de segurança de dados da indústria de cartões de pagamento e procedimentos da avaliação de segurança (PCI DSS)*. Preencha todas as seções: o comerciante é responsável por garantir que todas as seções sejam preenchidas pelas partes relevantes, se aplicável. Entre em contato com seu adquirente (banco do comerciante) ou empresas de pagamento para determinar os procedimentos de relatório e envio.

Parte 1. Informações sobre o comerciante e o avaliador de segurança qualificado

Parte 1a. Informações sobre a organização do comerciante

Nome da empresa:		DBA (fazendo negócios como):	
Contato:		Forma de tratamento:	
Telefone:		E-mail:	
Endereço comercial:		Cidade:	
Estado/província:		País:	
			CEP:
URL:			

Parte 1b. Informações sobre a empresa do assessor de segurança qualificado (se aplicável)

Nome da empresa:			
Nome do contato principal do QSA:		Forma de tratamento:	
Telefone:		E-mail:	
Endereço comercial:		Cidade:	
Estado/província:		País:	
			CEP:
URL:			

Parte 2. Resumo executivo

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

<input type="checkbox"/> Varejo	<input type="checkbox"/> Telecomunicações	<input type="checkbox"/> Armazéns e Supermercados
<input type="checkbox"/> Petróleo	<input type="checkbox"/> Comércio eletrônico	<input type="checkbox"/> Pedido por correio/telefone (MOTO)
<input type="checkbox"/> Outros (especificar):		

Quais tipos de canais de pagamento seu negócio atende?	Quais canais de pagamento são abrangidos por esse SAQ?
<input type="checkbox"/> Pedido por telefone/correio (MOTO)	<input type="checkbox"/> Pedido por telefone/correio (MOTO)
<input type="checkbox"/> Comércio eletrônico	<input type="checkbox"/> Comércio eletrônico
<input type="checkbox"/> Cartão presente (face a face)	<input type="checkbox"/> Cartão presente (face a face)

Observação: se sua organização tiver um processo ou canal de pagamento que não seja abrangido por

esse SAQ, consulte seu adquirente ou empresa de pagamento sobre a validação para outros canais.

Parte 2b. Descrição da indústria de cartões de pagamento

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

Parte 2c. Locais

Liste os tipos de instalação e um resumo dos locais (por exemplo, lojas de varejo, escritórios corporativos, centrais de dados, centrais de chamadas etc.) incluídos na revisão de PCI DSS.

Tipo de instalação	Número de instalações desse tipo	Local da instalação (cidade, país)
<i>Exemplo: Lojas de varejo</i>	3	<i>Boston, MA, EUA</i>

Parte 2d. Aplicativo de pagamento

A organização usa um ou mais dos aplicativos de pagamento? Sim Não

Forneça as seguintes informações relacionadas aos aplicativos de pagamento usados pela sua organização:

Nome do aplicativo de pagamento	Número da versão	Fornecedor do aplicativo	O aplicativo está listado no PA-DSS?	Data de expiração da listagem PA-DSS (se aplicável)
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	

Parte 2e. Descrição do ambiente

Forneça uma descrição de **alto nível** do ambiente abrangido por essa avaliação.

Por exemplo:

- *Conexões dentro e fora do ambiente de dados do titular do cartão (CDE).*
- *Os componentes de sistema críticos no CDE, como dispositivos POS, banco de dados, servidores da Web etc. e quaisquer outros componentes de pagamentos necessários, conforme aplicável.*

Seu negócio usa segmentação de rede para afetar o escopo do seu ambiente de PCI DSS?

(Consulte a seção "Segmentação de rede" do PCI DSS para obter orientação sobre a segmentação de rede)

Sim Não

Parte 2f. Prestadores de serviços de terceiros

Sua empresa usa um integrador e revendedor qualificado (QIR)?

Se sim:

Nome da empresa do QIR:

Nome do indivíduo QIR:

Descrição dos serviços prestados pelo QIR:

Sim Não

A sua empresa compartilha dados de titulares de cartão com qualquer provedor de serviços de terceiros (por exemplo, integrador e revendedor qualificado (QIR), gateways, processadores de pagamento, prestadores de serviços de pagamento (PSP), empresas de hospedagem de web, agentes de reserva de companhias aéreas, agentes do programa de fidelidade, etc.)?

Sim Não

Se sim:

Nome do prestador de serviço:

Descrição dos serviços fornecidos:

Nome do prestador de serviço:	Descrição dos serviços fornecidos:

Observação: o requisito 12.8 aplica-se a todas as entidades listadas.

Parte 2g. Qualificação para preencher o SAQ C

O comerciante certifica a qualificação de preenchimento desta versão abreviada do Questionário de autoavaliação porque, para esse canal de pagamento:

- O comerciante possui um sistema de aplicativo de pagamento e uma conexão com a internet no mesmo dispositivo e/ou na mesma rede local (LAN);
- O sistema de aplicativo de pagamento/dispositivo ligado à internet não está conectado a nenhum outro sistema dentro do ambiente do comerciante;
- O local físico do ambiente de POS não é conectado a outras instalações ou locais e qualquer LAN é somente para um local;
- O comerciante não armazena dados do titular do cartão em formato eletrônico; e
- Se o comerciante armazenar os dados do titular do cartão, esses dados só estarão em relatórios ou cópias em papel dos recibos e não serão recebidos eletronicamente.

Seção 2: Questionário de autoavaliação C

Observação: as perguntas a seguir estão numeradas de acordo com os requisitos e procedimentos de teste do PCI DSS, conforme definido no documento Requisitos do PCI DSS e procedimentos da avaliação de segurança.

Data de conclusão da autoavaliação:

Construir e manter a segurança de rede e sistemas

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

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
1.2 As configurações do firewall e do roteador restringem as conexões entre redes não confiáveis e qualquer sistema no ambiente de dados do titular do cartão, da seguinte forma: 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.					
1.2.1 (a) O tráfego de entrada e saída é restrito ao necessário para o ambiente de dados do titular do cartão?	<ul style="list-style-type: none"> Reveja o firewall e os padrões de configuração do roteador Examine o firewall e as configurações do roteador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Todos os outros tráfegos de entrada e saída são recusados de forma específica (como ao usar a opção explícita "recusar todos" ou uma recusa implícita após a declaração de permissão)?	<ul style="list-style-type: none"> Reveja o firewall e os padrões de configuração do roteador Examine o firewall e as configurações do roteador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
1.2.3	Existem firewalls de perímetro instalados entre quaisquer redes sem fio e o ambiente de dados do titular do cartão e esses firewalls estão configurados para recusar ou permitir (se esse tráfego for necessário para fins comerciais) apenas tráfegos autorizados a partir do ambiente sem fio no ambiente de dados do titular do cartão?	<ul style="list-style-type: none"> Reveja o firewall e os padrões de configuração do roteador Examine o firewall e as configurações do roteador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3	O acesso público direto é proibido entre a internet e qualquer componente do sistema no ambiente de dados do titular do cartão, da seguinte forma:					
1.3.4	O tráfego de saída do ambiente de dados do titular do cartão para a internet está explicitamente autorizado?	<ul style="list-style-type: none"> Examine o firewall e as configurações do roteador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	São permitidas apenas as conexões estabelecidas na rede?	<ul style="list-style-type: none"> Examine o firewall e as configurações do roteador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
2.1 (a) Os valores-padrão entregues pelo fornecedor são sempre alterados antes de instalar um sistema na rede? <i>Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando, às utilizadas pelos sistemas operacionais, softwares que fornecem serviços de segurança, aplicativos e contas do sistema, terminais de ponto de venda (POS), solicitações de pagamento, sequências de comunidade de Protocolo de Gerenciamento de Rede Simples (SNMP) etc.</i>	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Examine a documentação do fornecedor Observe as configurações do sistema e as definições da conta Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) As contas-padrão desnecessárias são removidas ou desativadas antes da instalação de um sistema na rede?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Reveja a documentação do fornecedor Examine as configurações do sistema e as definições da conta Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1 Para ambientes sem fio conectados ao ambiente dos dados do titular do cartão ou para a transmissão dos dados do titular do cartão, TODOS os padrões do fornecedor sem fio são alterados nas instalações, da seguinte forma:					
(a) As chaves de criptografia padrão são alteradas na instalação e são modificadas sempre que um funcionário que conhece as chaves sai da empresa ou troca de cargo?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Reveja a documentação do fornecedor Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) As strings de comunidades de SNMP padrão dos dispositivos sem fio são alteradas na instalação?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Reveja a documentação do fornecedor Entreviste a equipe Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
	(c) As senhas/frases de senha padrão dos pontos de acesso são alteradas na instalação?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Entreviste a equipe Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) O firmware dos dispositivos sem fio é atualizado para ser compatível com a criptografia robusta para autenticação e transmissão em redes sem fio?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Reveja a documentação do fornecedor Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(e) Os outros padrões relacionados à segurança do fornecedor de dispositivos sem fio são alterados, se aplicável?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Reveja a documentação do fornecedor Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2	(a) Os padrões de configuração são desenvolvidos para todos os componentes do sistema e estão de acordo com os padrões de fortalecimento do sistema aceitos pelo setor? <i>As fontes para os padrões de fortalecimento do sistema aceitas pelo setor incluem, entre outras, o SysAdmin Audit Network Security (SANS) Institute, o National Institute of Standards Technology (NIST), o International Organization for Standardization (ISO) e o Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> Reveja os padrões de configuração do sistema Reveja os padrões de fortalecimento aceitos pelo setor Reveja as políticas e procedimentos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os padrões de configuração do sistema são atualizados quando novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.1?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Os padrões de configuração do sistema são aplicados quando novos sistemas são configurados?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
(d) Os padrões de configuração do sistema incluem todos os seguintes itens: <ul style="list-style-type: none"> • Alteração de todos os padrões informados pelo fornecedor e eliminação de contas padrão desnecessárias? • Implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? • Habilitar apenas serviços, protocolos, daemons, etc. necessários, conforme exigido para a função do sistema? • Recursos de segurança adicionais são implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros? • Os parâmetros de segurança do sistema são configurados para impedir o uso incorreto? • Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários são removidas? 	<ul style="list-style-type: none"> ▪ Reveja os padrões de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1 (a) Há a implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? <i>Por exemplo, servidores da Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.</i>	<ul style="list-style-type: none"> ▪ Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Se forem usadas tecnologias de virtualização, somente uma função principal está implementada por componente ou dispositivo do sistema virtual?	<ul style="list-style-type: none"> ▪ Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
2.2.2	(a) Somente os serviços, protocolos e daemons necessários, entre outros, são ativados conforme a necessidade para a função do sistema (ou seja, os serviços e protocolos que não são diretamente necessários para a execução da função especificada do dispositivo estão desativados)?	<ul style="list-style-type: none"> Reveja os padrões de configuração Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Todos os protocolos, daemons ou serviços não seguros e ativados são justificados de acordo com os padrões de configuração documentados?	<ul style="list-style-type: none"> Reveja os padrões de configuração Entreviste a equipe Examine as definições de configuração Compare serviços ativos etc. com justificativas documentadas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Recursos de segurança adicionais são documentados e implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros? Observação: onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.	<ul style="list-style-type: none"> Reveja os padrões de configuração Examine as definições de configuração 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(a) Os administradores do sistema e/ou equipes que configuram os componentes do sistema estão bem-informados sobre as configurações comuns dos parâmetros de segurança para esses componentes do sistema?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) As configurações comuns dos parâmetros de segurança estão incluídas nos padrões de configuração do sistema?	<ul style="list-style-type: none"> Reveja os padrões de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) As configurações dos parâmetros de segurança estão definidas corretamente nos componentes do sistema?	<ul style="list-style-type: none"> Examine os componentes do sistema Examine as definições de parâmetro de segurança Compare as definições com os padrões de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
2.2.5	(a) Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários foram removidas?	<ul style="list-style-type: none"> Examine os parâmetros de segurança nos componentes do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) As funções ativadas estão documentadas e oferecem suporte para uma configuração segura?	<ul style="list-style-type: none"> Reveja a documentação Examine os parâmetros de segurança nos componentes do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Existem somente funcionalidades registradas presentes nos componentes do sistema?	<ul style="list-style-type: none"> Reveja a documentação Examine os parâmetros de segurança nos componentes do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Os acessos administrativos fora do console estão criptografados da seguinte forma: Observação: Onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.					
	(a) Todos os acessos administrativos fora do console são criptografados com criptografia robusta e um método de criptografia robusta é invocado antes da solicitação da senha do administrador?	<ul style="list-style-type: none"> Examine os componentes do sistema Examine as configurações do sistema Observe o logon de um administrador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os serviços do sistema e os arquivos de parâmetros são configurados para prevenir o uso de Telnet e outros comandos de logon remoto não seguros?	<ul style="list-style-type: none"> Examine os componentes do sistema Examine os serviços e arquivos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) O acesso do administrador às interfaces de gerenciamento baseadas na Web é criptografado com uma criptografia robusta?	<ul style="list-style-type: none"> Examine os componentes do sistema Observe o logon de um administrador 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Para a tecnologia em uso, a criptografia robusta é implementada de acordo com as melhores práticas do setor e/ou recomendações do fornecedor?	<ul style="list-style-type: none"> Examine os componentes do sistema Reveja a documentação do fornecedor Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
2.5	<p>Os procedimentos operacionais e as políticas de segurança para gerenciamento dos padrões do fornecedor e outros parâmetros de segurança são/estão:</p> <ul style="list-style-type: none"> ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas? 	<ul style="list-style-type: none"> ▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Proteger os dados do titular do cartão

Requisito 3: Proteger os dados armazenados do titular do cartão

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
3.2	(c) Os dados de autenticação confidenciais ou dados irrecuperáveis são excluídos ou restituídos após a conclusão do processo de autorização?	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos ▪ Examine as configurações do sistema ▪ Examine os processos de exclusão 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Todos os sistemas cumprem os seguintes requisitos em relação ao não armazenamento de dados de autenticação confidenciais após a autorização (mesmo se criptografados):					
3.2.1	<p>O conteúdo completo de qualquer rastreamento (da tarja magnética localizada na parte posterior do cartão ou qualquer dado equivalente presente em um chip ou em qualquer outro lugar) não é armazenado após a autorização?</p> <p><i>Esses dados também são denominados como rastreamento completo, rastreamento, rastreamento 1, rastreamento 2 e dados da tarja magnética.</i></p> <p>Observação: no curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser mantidos:</p> <ul style="list-style-type: none"> • O nome do titular do cartão • Número da conta primária (PAN) • Data de vencimento e • Código de serviço <p><i>Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.</i></p>	<ul style="list-style-type: none"> ▪ Examine as fontes de dados, incluindo: <ul style="list-style-type: none"> • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)				
		Sim	Sim com CCW	Não	N/D	
3.2.2	O código ou valor de verificação do cartão (número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) não é armazenado após a autorização?	<ul style="list-style-type: none"> ▪ Examine as fontes de dados, incluindo: <ul style="list-style-type: none"> • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Após a autorização, o número de identificação pessoal (PIN) ou o bloqueio de PIN criptografado não é armazenado?	<ul style="list-style-type: none"> ▪ Examine as fontes de dados, incluindo: <ul style="list-style-type: none"> • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3	O PAN é mascarado quando exibido (os primeiros seis e últimos quatro dígitos são o número máximo de dígitos a serem exibidos) de modo que somente funcionários com uma necessidade comercial legítima podem visualizar mais do que os seis primeiros/últimos quatro dígitos do PAN? <i>Observação: esse requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do titular do cartão, por exemplo, requisitos legais ou da bandeira do cartão de pagamento para recebimentos do ponto de venda (POS).</i>	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos ▪ Reveja as funções que precisam de acesso para exibições do PAN completo ▪ Examine as configurações do sistema ▪ Observe as exibições do PAN 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
4.1 (a) São usados protocolos de segurança e criptografia fortes para proteger dados sensíveis do titular do cartão durante a transmissão através de redes abertas e públicas? Observação: onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos. <i>Exemplos de redes abertas e públicas incluem, entre outros, internet, tecnologias sem fio, incluindo 802.11 e bluetooth, tecnologias de celular, por exemplo, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) e General Packet Radio Service (GPRS).</i>	<ul style="list-style-type: none"> Reveja os padrões documentados Reveja as políticas e procedimentos Reveja todos os locais em que o CHD é transmitido ou recebido Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) São aceitas apenas chaves e/ou certificados confiáveis?	<ul style="list-style-type: none"> Observe as transmissões de entrada e saída Examine as chaves e certificados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) São implementados protocolos de segurança para usar apenas configurações seguras e não apoiar versões ou configurações inseguras?	<ul style="list-style-type: none"> Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) A força da criptografia adequada foi implementada para a metodologia de criptografia em uso (verifique as recomendações/melhores práticas do fornecedor)?	<ul style="list-style-type: none"> Reveja a documentação do fornecedor Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) Para implementações de TLS, o TLS é habilitado sempre que dados de titulares de cartão são transmitidos ou recebidos? <i>Por exemplo, para implementações com base no navegador:</i> <ul style="list-style-type: none"> O "HTTPS" aparece como parte do protocolo de Universal Record Locator (URL) do navegador, e Os dados do titular do cartão são exigidos somente se o "HTTPS" aparece como parte do URL. 	<ul style="list-style-type: none"> Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
4.1.1	São usadas as melhores práticas da indústria para implementar criptografia forte para a autenticação e transmissão para as redes sem fio que transmitem dados de titulares de cartão ou que estão conectadas ao ambiente de dados do titular do cartão? <div style="background-color: #cccccc; height: 15px; width: 100%;"></div>	<ul style="list-style-type: none"> ▪ Reveja os padrões documentados ▪ Reveja as redes sem fio ▪ Examine as definições de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(b) Existem políticas em vigor que afirmam que os PANs desprotegidos não são enviados por meio das tecnologias de envio de mensagens de usuário final?	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Manter um programa de gerenciamento de vulnerabilidades

Requisito 5: Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
5.1	Os softwares antivírus estão implementados em todos os sistemas normalmente afetados por softwares mal-intencionados?	<ul style="list-style-type: none"> Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<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 (como vírus, trojans, worms, spywares, adwares e rootkits)?	<ul style="list-style-type: none"> Reveja a documentação do fornecedor Examine as configurações do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	São executadas avaliações periódicas para identificar e avaliar a evolução de ameaças de malware a fim de confirmar se tais sistemas continuam sendo considerados como não normalmente afetados por softwares mal-intencionados?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue:					
	(a) Todos os softwares antivírus e as definições são mantidos atualizados?	<ul style="list-style-type: none"> Examine as políticas e procedimentos Examine as configurações do antivírus, incluindo a instalação principal Examine os componentes do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) As atualizações automáticas e as varreduras periódicas estão ativadas e sendo executadas?	<ul style="list-style-type: none"> Examine as configurações do antivírus, incluindo a instalação principal Examine os componentes do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Todos os mecanismos de antivírus geram logs de auditoria e os logs são mantidos de acordo com o Requisito 10.7 do PCI DSS?	<ul style="list-style-type: none"> Examine as configurações do antivírus Reveja os processos de retenção de registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
5.3 Todos os mecanismos do antivírus: <ul style="list-style-type: none"> ▪ Estão sendo executados ativamente? ▪ Não podem ser desativados ou alterados pelos usuários? <p><i>Observação: as soluções antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período durante o qual a proteção antivírus não estiver ativa.</i></p>	<ul style="list-style-type: none"> ▪ Examine as configurações do antivírus ▪ Examine os componentes do sistema ▪ Observe os processos ▪ Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
<p>6.1 Há um processo para identificar vulnerabilidades de segurança, incluindo o seguinte:</p> <ul style="list-style-type: none"> ▪ Uso de origens externas conhecidas para obter informações sobre vulnerabilidade? ▪ Classificação de uma escala de risco para as vulnerabilidades, o que inclui identificação de todas as vulnerabilidades de "alto risco" e "críticas"? <p>Observação: as classificações de risco devem ser baseadas nas melhores práticas do setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.</p> <p>Os métodos para avaliar as vulnerabilidades e classificar o nível de risco variam com base no ambiente da organização e na estratégia de avaliação de risco. As classificações de risco devem, no mínimo, identificar todas as vulnerabilidades consideradas de "alto risco" ao ambiente. Além da classificação de risco, as vulnerabilidades podem ser consideradas "críticas" se apresentarem uma ameaça iminente ao ambiente, sistemas críticos de impacto e/ou resultariam em comprometimento potencial se não resolvidas. Exemplos de sistemas críticos podem incluir sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão.</p>	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os processos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
6.2	(a) Todos os componentes e softwares do sistema estão protegidos de vulnerabilidades conhecidas devido à instalação de patches de segurança aplicáveis disponibilizados pelo fornecedor?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os patches de segurança críticos são instalados no prazo de um mês após o lançamento? Observação: os patches de segurança crítica devem ser identificados de acordo com o processo de classificação de risco definido no Requisito 6.1.	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Examine os componentes do sistema Compare a lista de patches de segurança instalados com as listas de patches recentes do fornecedor 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	Após a conclusão de uma mudança significativa, são implementados todos os requisitos do PCI DSS em todos os sistemas novos ou alterados e redes, e atualizada a documentação conforme aplicável? Observação: este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.	<ul style="list-style-type: none"> Rastreie as alterações para alterar a documentação de controle Examine a documentação de controle de alteração Entreviste a equipe Observar os sistemas ou redes afetados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Implementar medidas rigorosas de controle de acesso

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

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
7.1	O acesso aos componentes do sistema e aos dados do titular do cartão é limitado somente àquelas pessoas cuja função requer tal acesso, conforme itens a seguir:					
7.1.2	O acesso aos IDs de usuários privilegiados é restrito ao seguinte: <ul style="list-style-type: none"> Restrito ao menor número de privilégios necessários para o desempenho das responsabilidades da função? Permitido apenas às funções que requerem especificamente tal acesso privilegiado? 	<ul style="list-style-type: none"> Examine a política escrita de controle de acesso Entreviste a equipe Entreviste os gerentes Reveja os IDs de usuários privilegiados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	É atribuído o acesso com base na classificação e função de trabalho do funcionário individualmente?	<ul style="list-style-type: none"> Examine a política escrita de controle de acesso Entreviste os gerentes Reveja os IDs dos usuários 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requisito 8: Identificar e autenticar o acesso aos componentes do sistema

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
8.1	Há procedimentos e políticas para os controles de gerenciamento de identificação de administradores e usuários que não são clientes em todos os componentes do sistema, como segue:				
8.1.1	Todos os usuários recebem um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do titular do cartão?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.5	(a) As contas são usadas por terceiros para acessar, suportar ou manter componentes do sistema via acesso remoto habilitado somente durante o período necessário e desativado quando não estiver em uso?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) As contas de acesso remoto de terceiros são monitoradas quando em uso?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.6	(a) As tentativas repetidas de acesso são limitadas bloqueando-se o ID do usuário após seis tentativas no máximo?				
8.1.7	Após o bloqueio da conta do usuário, 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"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.8	Se uma sessão ficar ociosa por mais de 15 minutos, o usuário é obrigado a se autenticar novamente (informar novamente a senha, por exemplo) para reativar o terminal ou a sessão?	<input type="checkbox"/>	<input type="checkbox"/>	<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"> ▪ Algo que você sabe, como uma senha ou frase de senha ▪ Algo que você tem, como um dispositivo de token ou um smart card ▪ Algo que você é, como a biométrica 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
8.2.3	<p>(a) Os parâmetros de senha do usuário são configurados para exigir que as senhas/frases de senha atendam ao seguinte?</p> <ul style="list-style-type: none"> Exigir um tamanho mínimo de senha de pelo menos sete caracteres Conter caracteres numéricos e alfabéticos <p>Alternativamente, as senhas/frases secretas devem ter complexidade e força pelo menos equivalentes aos parâmetros especificados acima.</p>	<ul style="list-style-type: none"> Examine as definições da configuração do sistema para verificar os parâmetros de senha 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	As senhas de usuário/frases secretas são alteradas pelo menos uma vez a cada 90 dias?	<ul style="list-style-type: none"> Reveja os procedimentos de senha Examine as definições de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.5	Um indivíduo deve criar uma nova senha/frase secreta diferente das últimas quatro senhas/frases de senha usadas?	<ul style="list-style-type: none"> Reveja os procedimentos de senha Amostra de componentes do sistema Examine as definições de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.6	As senhas/frases secretas são definidas com um valor exclusivo para cada usuário para a primeira utilização e após reiniciar, e cada usuário deve mudar sua senha imediatamente após o primeiro uso?	<ul style="list-style-type: none"> Reveja os procedimentos de senha Examine as definições de configuração do sistema Observe a equipe de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	<p>Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE é protegido usando a autenticação multifatores, conforme a seguir?</p> <p>Observação: a autenticação multifatores exige que um mínimo de dois dos três métodos de autenticação (ver Exigência 8.2 de PCI DSS para obter descrições dos métodos de autenticação) seja usado para autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifatores.</p>					

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
8.3.1 É incorporada autenticação multifatores para todos os acessos que não utilizam console no CDE para os funcionários com acesso administrativo? <i>Observação: este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.</i>	<ul style="list-style-type: none"> ▪ Examine as configurações do sistema ▪ Observar o administrador de pessoal registrando no CDE 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.2 É incorporada autenticação multifatores para todos os acessos de rede remota (usuário e administrador e incluindo o acesso de terceiros para suporte ou manutenção) provenientes de fora da rede da entidade?	<ul style="list-style-type: none"> ▪ Examine as configurações do sistema ▪ Observar os funcionários se conectando remotamente 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4 (a) Os procedimentos e políticas de autenticação são documentados e comunicados a todos os usuários?	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos ▪ Reveja o método de distribuição ▪ Entreviste a equipe ▪ Entreviste os usuários 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) As políticas e procedimentos de autenticação incluem o seguinte? <ul style="list-style-type: none"> • Orientação sobre selecionar credenciais fortes de autenticação • Orientação sobre como os usuários devem proteger suas credenciais de autenticação • Instruções para não reutilizar senhas anteriormente usadas • Instruções para os usuários de alteração da senha se houver suspeita de que ela possa estar comprometida 	<ul style="list-style-type: none"> ▪ Reveja as políticas e procedimentos ▪ Reveja a documentação fornecida aos usuários 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
8.5	<p>As contas e senhas (ou outros métodos de autenticação) de grupo, compartilhadas ou genéricas, são proibidas conforme os itens a seguir:</p> <ul style="list-style-type: none"> Os IDs e as contas de usuários genéricos são desativados ou removidos; Não existem IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas; e IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema? 	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Examine as listas de ID do usuário Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.8	<p>Os procedimentos operacionais e políticas de segurança para a identificação e autenticação são/estão:</p> <ul style="list-style-type: none"> Documentados Em uso Conhecidos por todas as partes envolvidas? 	<ul style="list-style-type: none"> Examine as políticas de segurança e procedimentos operacionais Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
9.1	Existem controles adequados em vigor para a entrada na instalação para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do titular do cartão?	<ul style="list-style-type: none"> Observe os controles de acesso físico Observe a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
9.1.1 (a) Existem câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis? <i>Observação: "áreas confidenciais" referem-se a qualquer central de dados, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam dados do titular do cartão. Isso exclui áreas voltadas ao público, onde apenas os terminais de ponto de venda estão presentes como as áreas de caixa em uma loja de varejo.</i>	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Observe os mecanismos de monitoramento físico Observe os recursos de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) As câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) são protegidos contra adulteração ou desabilitação?	<ul style="list-style-type: none"> Observe os processos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Os dados são coletados a partir de câmeras de vídeo e/ou mecanismos de controle de acesso revisados e correlacionados com outras entradas?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Entreviste a equipe de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Os dados são coletados de câmeras de vídeo e/ou mecanismos de controle de acesso armazenados por pelo menos três meses, menos em caso contrário restrito por lei?	<ul style="list-style-type: none"> Reveja os processos de retenção de dados Observe o armazenamento de dados Entreviste a equipe de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.2 Os controles físicos e/ou lógicos são usados para restringir o acesso a pontos de rede acessíveis publicamente? <i>Por exemplo, pontos de rede localizados em áreas públicas e áreas acessíveis a visitantes podem ser desativados e somente ativados quando o acesso à rede é explicitamente autorizado. Alternativamente, processos podem ser implementados para garantir que os visitantes sempre sejam acompanhados nas áreas com pontos de rede ativos.</i>	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Entreviste a equipe Observe os locais 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
9.5	Todas as mídias estão fisicamente seguras (incluindo, entre outros, computadores, mídias eletrônicas removíveis, recibos em papel, relatórios em papel e faxes)? <i>Para os fins do requisito 9, "mídia" refere-se a todas as mídias em papel ou eletrônicas que contêm dados do titular do cartão.</i>	<ul style="list-style-type: none"> Reveja as políticas e procedimentos para segurança física das mídias Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos para distribuição de mídia 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os controles incluem o seguinte:					
9.6.1	A mídia é classificada para que a confidencialidade dos dados possa ser determinada?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos para classificação de mídia Entreviste a equipe de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	A mídia é enviada via um mensageiro seguro ou outro método de entrega que possa ser rastreado com precisão?	<ul style="list-style-type: none"> Entreviste a equipe Examine a documentação e registros de rastreamento da distribuição de mídia 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	A aprovação gerencial é obtida antes de mover as mídias (especialmente quando a mídia é distribuída a pessoas)?	<ul style="list-style-type: none"> Entreviste a equipe Examine a documentação e registros de rastreamento da distribuição de mídia 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) Todas as mídias são destruídas quando não são mais necessárias por razões corporativas ou legais?	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de destruição periódica de mídias 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) A destruição é executada da seguinte forma:					

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
9.8.1	(a) Os materiais impressos são fragmentados, incinerados ou reciclados, de forma que os dados do titular do cartão não possam ser reconstruídos?	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de destruição periódica de mídias Entreviste a equipe Observe os processos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os contêineres usados para materiais que armazenam informações são destruídos de forma segura para prevenir o acesso aos conteúdos?	<ul style="list-style-type: none"> Examine a segurança dos contêineres de armazenamento 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	<p>Os dispositivos que capturam os dados do cartão de pagamento por meio de interação física direta com o cartão são protegidos contra falsificação e substituição como segue?</p> <p>Observação: esse requisito é aplicável aos dispositivos de leitura do cartão usados em transações com a presença do cartão (ou seja, de passar ou inserir) no ponto de venda. Este requisito não tem o objetivo de se aplicar aos componentes de entrada de chave manual, como teclados de computador e teclados POS.</p>					
	(a) As políticas e procedimentos exigem que uma lista de tais dispositivos seja mantida?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) As políticas e procedimentos exigem que os dispositivos sejam periodicamente inspecionados quanto à falsificação ou substituição?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) As políticas e procedimentos exigem que os funcionários sejam treinados para reconhecer os comportamentos suspeitos e para reportar a falsificação ou substituição de dispositivos?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1	<p>(a) A lista de dispositivos inclui o seguinte?</p> <ul style="list-style-type: none"> Marca, modelo do dispositivo Localização do dispositivo (por exemplo, o endereço do local ou instalação onde o dispositivo está localizado) Número de série do dispositivo ou outro método de identificação exclusivo 	<ul style="list-style-type: none"> Examine a lista de dispositivos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
	(b) Essa lista é precisa e está atualizada?	<ul style="list-style-type: none"> Observar os dispositivos e locais de dispositivos e comparar a lista 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Essa lista de dispositivos é atualizada quando dispositivos são adicionados, realocados, retirados de serviço etc?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2	<p>(a) As superfícies dos dispositivos são inspecionadas periodicamente para detectar falsificação (por exemplo, adição de espões aos dispositivos) ou substituição (por exemplo, verificando o número de série ou outras características do dispositivo para verificar se ele não foi trocado por um dispositivo fraudulento) como segue?</p> <p>Observação: exemplos de sinais de que um dispositivo possa ter sido adulterado ou substituído incluem apêndices inesperados ou cabos conectados ao dispositivo, rótulos de segurança alterados ou ausentes, revestimento quebrado ou de cor diferente, ou alterações no número de série ou outras marcas externas.</p>	<ul style="list-style-type: none"> Entreviste a equipe Observe os processos de inspeção e compare-os com os processos definidos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os funcionários estão cientes dos procedimentos de inspeção dos dispositivos?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
9.9.3 Os funcionários são treinados para reconhecer tentativas de falsificação ou substituição de dispositivos para incluir o seguinte?					
(c) Os materiais de treinamento para os funcionários nos locais dos pontos de venda incluem o seguinte? <ul style="list-style-type: none"> • Verifique a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos. • Não instale, substitua ou devolva dispositivos sem verificação. • Esteja atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas). • Reporte comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança). 	<ul style="list-style-type: none"> ▪ Reveja os materiais de treinamento 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Os funcionários dos locais dos pontos de venda receberam treinamento e conhecem os procedimentos para detectar e reportar tentativas de falsificação ou substituição de dispositivos?	<ul style="list-style-type: none"> ▪ Entrevista as equipes nos locais de POS 	<input type="checkbox"/>	<input type="checkbox"/>	<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 titular do cartão*

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
10.2	Foram implementadas trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:					
10.2.2	Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Tentativas de acesso lógico inválidas?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.5	Há uso e alterações dos mecanismos de identificação e autenticação, incluindo, entre outros, a criação de novas contas e aumento de privilégios e todas as alterações, adições ou exclusões de contas com privilégios raiz ou administrativos?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	As seguintes entradas da trilha de auditoria são registradas para todos os componentes do sistema em cada um dos eventos a seguir?					
10.3.1	Identificação do usuário?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
10.3.2	Tipo de evento?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.3	Data e hora?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	Indicação de sucesso ou falha?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	Origem do evento?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identidade ou nome dos dados, componentes do sistema ou recursos afetados?	<ul style="list-style-type: none"> ▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	<p>Os logs e ocorrências de segurança para todos os componentes do sistema são revisados para identificar irregularidades ou atividades suspeitas como segue?</p> <p>Observação: as ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6</p>					

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
10.6.1 (b) Os seguintes logs e ocorrências de segurança são revisados, no mínimo, diariamente, de modo manual ou por ferramentas de log? <ul style="list-style-type: none"> Todas as ocorrências de segurança Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD Logs de todos os componentes críticos do sistema Logs de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do comércio eletrônico, etc.) 	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de segurança Observe os processos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2 (b) Os logs de todos os outros componentes do sistema são revisados periodicamente, de modo manual ou por ferramentas de log, com base na estratégia de gerenciamento de risco e nas políticas da organização?	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de segurança Reveja a documentação de avaliação de risco Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3 (b) Há um acompanhamento das exceções e irregularidades identificadas durante o processo de revisão?	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de segurança Observe os processos Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7 (b) Os logs de auditoria são retidos pelo menos uma vez ao ano?	<ul style="list-style-type: none"> Reveja os procedimentos e políticas de segurança Entreviste a equipe Examine os logs de auditoria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Ao menos os últimos três meses de logs estão imediatamente disponíveis para análise?	<ul style="list-style-type: none"> Entreviste a equipe Observe os processos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requisito 11: Testar regularmente os sistemas e processos de segurança

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
11.1 (a) Processos para detecção e identificação dos pontos de acesso sem fio não autorizados e autorizados são implementados trimestralmente? Observação: métodos que podem ser usados no processo incluem, entre outros, varreduras de rede sem fio, inspeções físicas/lógicas de componentes e infraestrutura do sistema, controle de acesso à rede (NAC) ou IDS/IPS sem fio. Qualquer método usado deve ser suficiente para detectar e identificar qualquer dispositivo não autorizado.	<ul style="list-style-type: none"> Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) A metodologia detecta e identifica qualquer ponto de acesso sem fio não autorizado, incluindo ao menos os itens a seguir? <ul style="list-style-type: none"> Cartões WLAN inseridos nos componentes do sistema; Dispositivos móveis ou portáteis fixados a componentes do sistema para criar um ponto de acesso sem fio (por exemplo, por USB, etc.); e Dispositivos sem fio conectados a uma porta de rede ou a um dispositivo de rede. 	<ul style="list-style-type: none"> Avalie a metodologia 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Se a varredura sem fio for utilizada para identificar os pontos de acesso sem fio autorizados e não autorizados, a varredura é executada pelo menos trimestralmente para todos os componentes e instalações do sistema?	<ul style="list-style-type: none"> Examine o resultado das varreduras sem fio recentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Se o monitoramento automatizado for utilizado (como IDS/IPS sem fio, NAC etc.), ele está configurado para gerar alertas à equipe?	<ul style="list-style-type: none"> Examine as definições de configuração 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.1 Um inventário de pontos de acesso sem fio autorizados é mantido e uma justificativa comercial é documentada para todos os pontos de acesso sem fio autorizados?	<ul style="list-style-type: none"> Examine os registros do inventário 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
11.1.2	(a) O plano de resposta a incidentes define e exige uma resposta em caso de detecção de ponto de acesso sem fio não autorizado?	<ul style="list-style-type: none"> Examine o plano de resposta a incidentes (veja o Requerimento 12.10) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) São tomadas ações quando os pontos de acesso sem fio não autorizados são encontrados?	<ul style="list-style-type: none"> Entreviste a equipe responsável Inspecione as varreduras sem fio recentes e as respostas relacionadas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>São executadas varreduras das vulnerabilidades das redes internas e externas pelo menos trimestralmente e após qualquer alteração significativa na rede (como instalações de novos componentes do sistema, alterações na topologia da rede, modificações das normas do firewall, upgrades de produtos) da seguinte forma?</p> <p>Observação: vários relatórios de varredura podem ser combinados no processo de varredura trimestral para mostrar que todos os sistemas foram mapeados e que todas as vulnerabilidades aplicáveis foram resolvidas. Pode ser exigida uma documentação adicional para verificar se as vulnerabilidades não resolvidas estão em processo de serem solucionadas.</p> <p>Para a conformidade inicial com o PCI DSS, não é necessário que as quatro varreduras trimestrais aprovadas sejam concluídas se o assessor verificar que 1) o resultado da varredura mais recente foi uma varredura aprovada, 2) a entidade possui políticas e procedimentos documentados que requerem a sequência de varreduras trimestrais e 3) as vulnerabilidades observadas nos resultados da varredura tenham sido corrigidas conforme mostrado em uma nova varredura. Nos anos seguintes após a análise inicial do PCI DSS, quatro varreduras trimestrais aprovadas devem ter ocorrido.</p>					

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
11.2.1	(a) As varreduras das vulnerabilidades internas são executadas trimestralmente?	<ul style="list-style-type: none"> Reveja os relatórios de varredura 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) O processo de varredura interna trimestral trata todas as vulnerabilidades de "alto risco" e inclui novas varreduras para verificar se todas as vulnerabilidades de "alto risco" (conforme definido pela Exigência 6.1 de PCI DSS) são resolvidas?	<ul style="list-style-type: none"> Reveja os relatórios de varredura 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) As varreduras são executadas trimestralmente por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2	(a) As varreduras das vulnerabilidades externas são executadas trimestralmente? <i>Observação: as varreduras externas trimestrais de vulnerabilidades devem ser realizadas por um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da indústria de cartões de pagamento (PCI SSC). Consulte o Guia do programa ASV publicado no site do PCI SSC para saber sobre responsabilidades de varredura do cliente, preparação de varredura etc.</i>	<ul style="list-style-type: none"> Reveja os resultados dos quatro últimos trimestres quanto às varreduras de vulnerabilidades externas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Os resultados da varredura externa trimestral cumprem os requisitos do <i>Guia do programa ASV</i> (por exemplo, nenhuma vulnerabilidade classificada com valor 4 ou superior pelo CVSS e nenhuma falha automática)?	<ul style="list-style-type: none"> Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) As varreduras de vulnerabilidades externas trimestrais são executadas por um fornecedor de varredura aprovado (ASV) pela PCI SSC?	<ul style="list-style-type: none"> Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
11.2.3 (a) Varreduras internas e externas e novas varreduras são realizadas, se necessário, após qualquer mudança significativa? <i>Observação: as varreduras devem ser realizadas por uma equipe qualificada.</i>	<ul style="list-style-type: none"> Examine e correlacione a documentação de controle de alteração e os relatórios de varredura 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) O processo de varredura inclui novas varreduras até que: <ul style="list-style-type: none"> Não existam vulnerabilidades com pontuação de 4 ou mais pelo CVSS para varreduras externas Um resultado aprovado seja obtido ou todas as vulnerabilidades definidas como "alto risco", conforme definido no Requisito 6.1 do PCI DSS, estejam solucionadas (para varreduras internas)? 	<ul style="list-style-type: none"> Reveja os relatórios de varredura 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) As varreduras são executadas por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	<ul style="list-style-type: none"> Entreviste a equipe 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4 Se a segmentação é usada para isolar o CDE de outras redes:					
(a) São definidos procedimentos de teste de penetração para testar todos os métodos de segmentação, para confirmar que eles estão operacionais e eficientes e que isolam-se todos os sistemas fora de escopo dos sistemas no CDE?	<ul style="list-style-type: none"> Examine os controles de segmentação Reveja a metodologia de teste de penetração 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
(b) O teste de penetração para verificar os controles de segmentação atende ao seguinte? <ul style="list-style-type: none"> • É executado pelo menos uma vez ao ano e após qualquer mudança nos métodos/controles da segmentação • Abrange todos os métodos/controles da segmentação em uso • Verifica se os métodos de segmentação estão operacionais e eficientes e isola todos os sistemas fora de escopo dos sistemas no CDE. 	<ul style="list-style-type: none"> ▪ Examine os resultados do teste mais recente de penetração 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(C) São executados testes por um recurso interno qualificado ou um terceiro externo qualificado e, conforme aplicável, há uma independência organizacional do testador (não é necessário que seja um QSA ou ASV)?	<ul style="list-style-type: none"> ▪ Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5 (a) Existe um mecanismo de detecção de mudança (por exemplo, ferramentas de monitoramento de integridade de arquivo) implementado para detectar modificações não autorizadas (incluindo as alterações, adições e exclusões) de arquivos críticos de sistema, arquivos de configuração ou arquivos de conteúdo? <p><i>Os exemplos de arquivos que devem ser monitorados incluem:</i></p> <ul style="list-style-type: none"> • Executáveis do sistema • Executáveis dos aplicativos • Arquivos de configuração e parâmetro • Arquivos de log e auditoria, históricos ou arquivados, armazenados centralmente • Arquivos críticos adicionais determinados pela entidade (por exemplo, por meio de avaliação de risco ou outros meios) 	<ul style="list-style-type: none"> ▪ Observe as definições do sistema e os arquivos monitorados ▪ Examine as definições de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
	<p>(b) O mecanismo de detecção de mudança é configurado para alertar os funcionários sobre modificação não autorizada (incluindo as alterações, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo, e as ferramentas realizam comparações de arquivos críticos pelo menos semanalmente?</p> <p>Observação: para fins de detecção de alterações, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Os mecanismos de detecção de alterações, como produtos de monitoramento da integridade dos arquivos, normalmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para os aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).</p>	<ul style="list-style-type: none"> Observe as definições do sistema e os arquivos monitorados Reveja os resultados das atividades de monitoramento 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5.1	Há um processo implementado para responder a qualquer alerta gerado pela solução de detecção de alterações?	<ul style="list-style-type: none"> Examine as definições de configuração do sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<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 todas as equipes

Observação: para as finalidades do Requisito 12, "equipe" refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias, e prestadores de serviços e consultores que "residem" no endereço da entidade ou têm acesso ao ambiente de dados do titular do cartão.

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada para todas as equipes relevantes?	<ul style="list-style-type: none"> Reveja a política de segurança de informações 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	A política de segurança é revisada ao menos uma vez por ano e atualizada quando o ambiente é alterado?	<ul style="list-style-type: none"> Reveja a política de segurança de informações Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	<p>O uso de políticas de tecnologias críticas é desenvolvido para definir o uso apropriado destas tecnologias e exige o seguinte:</p> <p>Observação: exemplos de tecnologias críticas incluem, entre outros, tecnologias de acesso remoto e sem fio, laptops, tablets, mídia eletrônica removível, uso de e-mails e da internet.</p>					
12.3.1	Aprovação explícita pelas partes autorizadas para uso das tecnologias?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Autenticação para o uso da tecnologia?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	Uma lista de todos esses dispositivos e equipes com acesso?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Usos aceitáveis das tecnologias?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Locais de rede aceitáveis para as tecnologias?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
12.3.8	Desconexão automática das sessões para tecnologias de acesso remoto após um período específico de inatividade?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	Ativação de tecnologias de acesso remoto para fornecedores e parceiros de negócio somente quando lhes for necessário, com desativação imediata após o uso?	<ul style="list-style-type: none"> Reveja as políticas de uso Entreviste a equipe responsável 	<input type="checkbox"/>	<input type="checkbox"/>	<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 todas as equipes?	<ul style="list-style-type: none"> Reveja os procedimentos e política de segurança Entreviste alguns dos funcionários responsáveis 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5	(b) As seguintes responsabilidades do gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e para as equipes que:					
12.5.3	Estabelecem, documentam e distribuem procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?	<ul style="list-style-type: none"> Reveja os procedimentos e a política de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) Existe um programa de conscientização de segurança formal para tornar todos os funcionários conscientes da política e dos procedimentos de segurança dos dados dos titulares de cartão?	<ul style="list-style-type: none"> Reveja o programa de conscientização de segurança 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	As políticas e procedimentos são mantidos e implementados para gerenciar os prestadores de serviços com os quais os dados do titular do cartão são compartilhados, ou que possam afetar a segurança dos dados, conforme segue:					
12.8.1	É mantida uma lista dos prestadores de serviços, incluindo uma descrição dos serviços prestados?	<ul style="list-style-type: none"> Reveja as políticas e procedimentos Observe os processos Reveja a lista de prestadores de serviço 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)				
		Sim	Sim com CCW	Não	N/D	
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 que eles possuem do titular do cartão, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente? Observação: as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.	<ul style="list-style-type: none"> Observe os acordos por escrito Reveja as políticas e procedimentos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Existe um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação?	<ul style="list-style-type: none"> Observe os processos Reveja as políticas e procedimentos e os documentos de suporte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	É mantido um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços?	<ul style="list-style-type: none"> Observe os processos Reveja as políticas e procedimentos e os documentos de suporte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	As informações mantidas sobre os requisitos do PCI DSS são administradas por cada prestador de serviços e quais são administradas pela entidade?	<ul style="list-style-type: none"> Observe os processos Reveja as políticas e procedimentos e os documentos de suporte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
12.10.1 (a) Foi criado um plano de resposta a incidentes para ser implementado em caso de violação do sistema?	<ul style="list-style-type: none"> ▪ Reveja o plano de resposta a incidentes ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) No mínimo, o plano aborda o seguinte:					
<ul style="list-style-type: none"> • Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo, no mínimo, a notificação às bandeiras? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Procedimentos de resposta específicos a incidentes? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Procedimentos de recuperação e continuidade dos negócios? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Processos de backup dos dados? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Análise dos requisitos legais para divulgação dos comprometimentos? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Abrangência e respostas de todos os componentes críticos do sistema? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras? 	<ul style="list-style-type: none"> ▪ Reveja os procedimentos do plano de resposta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apêndice A: Requisitos adicionais do PCI DSS

Anexo A1: *Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada*

Esse apêndice não é usado para avaliações de comerciante.

Anexo A2: *Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS*

Pergunta do PCI DSS		Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
			Sim	Sim com CCW	Não	N/D
A2.1	<p><i>Para terminais POS POI (e os pontos de terminação SSL/TLS ao qual eles se conectam) usando SSL e/ou TLS precoce:</i></p> <ul style="list-style-type: none"> Os dispositivos são confirmados para não serem suscetíveis a qualquer façanha conhecida para SSL/TLS precoce <p><i>Ou:</i></p> <ul style="list-style-type: none"> Há um plano formal de redução de riscos e migração em vigor de acordo com a exigência 2.2? 	<ul style="list-style-type: none"> Revise a documentação (por exemplo, documentação do fornecedor, detalhes de configuração do sistema/rede etc.) que verifica que dispositivos POI POS não são suscetíveis a qualquer vulnerabilidade conhecida para SSL/TLS precoce 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pergunta do PCI DSS	Teste esperado	Resposta (Marque uma resposta para cada pergunta)			
		Sim	Sim com CCW	Não	N/D
<p>A2.2 Existe um plano formal de redução de riscos e migração em vigor para todas as implementações que usam SSL ou TLS precoce (exceto conforme permitido em A2.1), que inclui:</p> <ul style="list-style-type: none"> ▪ Descrição de uso, incluindo dados que estão sendo transmitidos, tipos e número de sistemas que usam e/ou suporte SSL/TLS precoce, tipo de ambiente; ▪ Resultados da avaliação de riscos e controles de redução de risco no lugar; ▪ Descrição dos processos para monitorar as novas vulnerabilidades associadas com SSL/TLS precoce; ▪ Descrição de processos de controle de alterações que são implementados para garantir que a SSL/TLS precoce não seja implementada em novos ambientes; ▪ Visão geral do plano do projeto de migração, incluindo a data de conclusão do objetivo da migração até no máximo 30 de junho de 2018? 	<ul style="list-style-type: none"> ▪ Rever o plano de redução de riscos e migração documentado 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apêndice A3: Validação Suplementar de Entidades Designadas (DESV)

Este Apêndice só se aplica a entidades designadas por uma empresa de pagamento ou adquirente conforme exigir uma validação adicional dos requisitos existentes de PCI DSS. Entidades que tenham necessidade de validar este Apêndice devem usar o modelo de relatório suplementar DESV e atestado suplementar de conformidade para relatórios e consultar a empresa de pagamento e/ou o adquirente aplicáveis sobre os procedimentos de submissão.

Apêndice B: Planilha dos controles de compensação

Use essa planilha para definir os controles de compensação para requisitos em que "SIM com CCW" foi selecionado.

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.

Consulte os Apêndices B, C e D do PCI DSS para obter informações sobre os controles de compensação e orientação sobre como preencher essa planilha.

Número e definição do requisito:

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

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

Este AOC é baseado em resultados observados no SAQ C (Seção 2), datado de (data de conclusão de SAQ).

Com base nos resultados documentados no SAQ C observados acima, os signatários identificados nas Partes 3b-3d, conforme aplicável, afirmam o seguinte estado de conformidade para a entidade identificada na Parte 2 desse documento: (**selecione um**):

<input type="checkbox"/>	<p>Em conformidade: todas as seções do SAQ do PCI DSS estão preenchidas e todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de CONFORMIDADE, de forma que a (nome da empresa do comerciante) demonstrou conformidade integral com o PCI DSS.</p>						
<input type="checkbox"/>	<p>Não conformidade: nem todas as seções do SAQ do PCI DSS estão preenchidas ou nem todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de NÃO CONFORMIDADE, de forma que a (nome da empresa do comerciante) não demonstrou conformidade integral com o PCI DSS.</p> <p>Data prevista para conformidade:</p> <p>A entidade que estiver enviando este formulário com um status de Não conformidade talvez tenha de preencher o Plano de ação na Parte 4 deste documento. <i>Verifique junto ao seu adquirente ou à(s) empresa(s) de pagamento antes de preencher a Parte 4.</i></p>						
<input type="checkbox"/>	<p>Em conformidade, mas com exceção legal: um ou mais dos requisitos foram marcados como "não" devido a uma restrição legal que evita que o requisito seja atendido. Essa opção exige revisão adicional do adquirente ou empresa de pagamento.</p> <p><i>Se selecionada, preencha o seguinte:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Requisito afetado</th> <th>Detalhes de como a restrição legal evita que o requisito seja atendido</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Requisito afetado	Detalhes de como a restrição legal evita que o requisito seja atendido				
Requisito afetado	Detalhes de como a restrição legal evita que o requisito seja atendido						

Parte 3a. Reconhecimento do status

O(s) signatário(s) confirma(m):
(Selecione todos os aplicáveis)

<input type="checkbox"/>	O Questionário de autoavaliação C do PCI DSS, versão (versão do SAQ), foi preenchido segundo as instruções nele contidas.
<input type="checkbox"/>	Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação em todos os aspectos materiais.
<input type="checkbox"/>	Eu confirmei com meu fornecedor do aplicativo de pagamento que o aplicativo não armazena dados de autenticação confidenciais após a autorização.
<input type="checkbox"/>	Eu li o PCI DSS e reconheço que sempre devo manter a conformidade total com o PCI DSS, conforme aplicável para o meu ambiente.
<input type="checkbox"/>	Se meu ambiente mudar, reconheço que devo reavaliá-lo e implementar quaisquer requisitos adicionais de PCI DSS que forem aplicáveis.

Parte 3a. Reconhecimento do status (continuação)

- | | |
|--------------------------|--|
| <input type="checkbox"/> | Não há evidências de armazenamento de dados da tarja magnética ¹ , dados de CAV2, CVC2, CID ou CVV2 ² , ou dados de PIN ³ depois da autorização da transação em QUAISQUER sistemas analisados durante essa avaliação. |
| <input type="checkbox"/> | As varreduras ASV estão sendo concluídas pelo fornecedor de varredura aprovado do PCI SSC (<i>nome do ASV</i>) |

Parte 3b. Atestado do comerciante

Assinatura do responsável executivo pelo comerciante ↑

Data:

Nome do responsável executivo pelo comerciante:

Forma de tratamento:

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

Se um QSA foi incluído ou auxiliado nessa avaliação, descreva a função executada:

Assinatura do funcionário devidamente autorizado da empresa do QSA ↑

Data:

Nome do funcionário devidamente autorizado:

Empresa do QSA:

Parte 3d. Envolvimento do Assessor de Segurança Interno (ISA) (se aplicável)

Se um ISA for envolvido ou auxiliado com esta avaliação, identificar o funcionário ISA e descrever o papel realizado:

¹ Dados criptografados na tarja magnética ou dados equivalentes em um chip usados para autorização durante a transação com o cartão. As entidades não podem reter esses dados de tarja magnética após a autorização da transação. Os únicos elementos dos dados da tarja magnética que podem ser retidos são o número da conta principal (PAN), o nome do titular do cartão e a data de vencimento.

² O valor de três ou quatro dígitos impresso no painel de assinatura ou na frente do cartão de pagamento usado para verificar transações com cartão não presente.

³ Número de identificação pessoal inserido pelo titular do cartão durante uma transação com cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

Parte 4. Plano de ação para requisitos que não estão em conformidade

Selecione a resposta apropriada para "Conformidade com os requisitos PCI DSS" 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 junto ao seu adquirente ou à(s) empresa(s) de pagamento antes de preencher a Parte 4.

Requisito do PCI DSS*	Descrição do requisito	Em conformidade com os requisitos do PCI DSS (selecione um)		Data de reparação e ações (se "NÃO" estiver selecionado para qualquer requisito)
		SIM	NÃO	
1	Instalar e manter uma configuração de firewall para proteger os dados do titular 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 titular do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
4	Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteger todos os sistemas contra malware e atualizar regularmente programas ou software de 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 titular do cartão de acordo com a necessidade de conhecimento para o negócio	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identificar e autenticar o acesso aos componentes do sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir o acesso físico aos dados do titular 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 titular 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 da informação para todas as equipes	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A2	Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS	<input type="checkbox"/>	<input type="checkbox"/>	

* Os Requisitos do PCI DSS indicados aqui referem-se às perguntas na Seção 2 do SAQ.

