Indústria de cartões de pagamento (PCI)
Padrão de segurança de dados

Questionário de autoavaliação D e Atestado de conformidade para comerciantes

Todos os outros comerciantes elegíveis a SAQ

Para uso com o PCI DSS versão 3.2

Revisão 1.1

Janeiro de 2017

Alterações no documento

Data	Versão de 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 2015	3.1		Atualizado para alinhar-se com a versão 3.1 do PCI DSS. Para detalhes das mudanças de PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.0 para 3.1*.
Julho de 2015	3.1	1.1	Atualizado para remover as referências às "melhores práticas", antes de 30 de Junho de 2015 e remover a opção de relatórios de versão 2 de PCI DSS para Requisito 11.3.
Abril de 2016	3.2	1.0	Atualizado para alinhar-se com o PCI DSS v 3.2. Para detalhes das alterações de PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.1 para 3.2*.
Janeiro de 2017	3.2	1.1	Enumeração da versão atualizada para alinhar-se com outros SAQs

TERMO DE RECONHECIMENTO:

A versão em inglês deste documento, conforme disponibilizada no site da PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês, a versão em inglês disponibilizada no local mencionado prevalecerá.

Índice

Antes de você começar

O SAQ D para comerciantes aplica-se aos comerciantes elegíveis a SAQ que não atendem aos critérios de qualquer outro SAQ. Exemplos de ambientes de comerciante que podem usar o SAQ D podem incluir, entre outros:

- Comerciantes de comércio eletrônico que aceitem dados do portador do cartão em seu site.
- Comerciantes com armazenamento eletrônico dos dados do portador do cartão
- Comerciantes que não armazenam eletronicamente dados do portador do cartão, mas que não atendem aos critérios de nenhum outro tipo de SAQ
- Comerciantes com ambientes que podem atender aos critérios de outro tipo de SAQ, mas que possuem requisitos de PCI DSS adicionais aplicáveis ao seu ambiente

Apesar de várias organizações que preenchem o SAQ D precisarem validar a conformidade com todos os requisitos do PCI DSS, algumas organizações com modelos de negócio bastante específicos podem descobrir que alguns requisitos não se aplicam. Consulte a orientação abaixo para obter informações sobre a exclusão de alguns requisitos específicos.

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 se seu ambiente está adequadamente dentro do escopo e atende aos critérios de elegibilidade para o SAQ que você está usando.
3. Avalie seu ambiente quanto à conformidade com os requisitos de PCI DSS.
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 D)
   - 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 *(Requisitos dos padrões de segurança de dados do PCI e Procedimentos de avaliação da segurança)*	• 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

Documento	Inclui:
Documentos de instruções e diretrizes do SAQ	• Informações sobre todos os SAQs e seus critérios de elegibilidade • Como determinar qual SAQ é o correto para a sua organização
Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS	• 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/A (Não disponível)	O requisito não é aplicável ao ambiente da organização (consulte a *Orientação para não aplicabilidade de determinados requisitos específicos* abaixo para ver exemplos). Todas as respostas nessa coluna exigem uma explicação de suporte no Apêndice C do SAQ.
Não testado	O requisito não foi incluído para consideração na avaliação e também não foi testado de nenhum modo. (Consulte *Entendendo a diferença entre Não aplicável e Não testado* abaixo para obter exemplos de quando essa opção deve ser usada).

	Todas as respostas nessa coluna exigem uma explicação de suporte no Apêndice D do SAQ.

Orientação para não aplicabilidade de determinados requisitos específicos

Apesar de várias organizações que preenchem o SAQ D precisarem validar a conformidade com todos os requisitos do PCI DSS, algumas organizações com modelos de negócio bastante específicos podem descobrir que alguns requisitos não se aplicam. Por exemplo, não se espera que uma empresa que não usa tecnologia sem fio de forma alguma valide a conformidade com as seções do PCI DSS que são específicas da tecnologia sem fio. De modo semelhante, uma organização que não armazena eletronicamente dados do titular do cartão não precisará validar os requisitos relacionados ao armazenamento seguro dos dados do titular do cartão (por exemplo, Requisito 3.4).

Exemplos de requisitos com aplicabilidade específica incluem:

- As perguntas específicas relacionadas à segurança das tecnologias sem fio (por exemplo: os Requisitos 1.2.3, 2.1.1 e 4.1.1) somente precisam ser respondidas se a função sem fio estiver presente em qualquer local da sua rede. 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.
- As questões específicas para desenvolvimento de aplicativos e códigos seguros (Requisitos 6.3 e 6.5) só precisarão ser respondidas se sua organização desenvolver seus próprios aplicativos personalizados.
- As perguntas dos Requisitos 9.1.1 e 9.3 só precisarão ser respondidas para instalações com “áreas confidenciais”, conforme definidas aqui. "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 as áreas que possuem somente terminais de pontos de vendas, como as áreas dos caixas em uma loja de varejo, mas inclui salas de servidores de back-office de lojas de varejo que armazenam dados do titular do cartão e áreas de armazenamento para grandes quantidades de dados do titular do cartão.

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".

Entendendo a diferença entre Não aplicável e Não testado

Requisitos considerados como não aplicáveis a um ambiente devem ser verificados como tal. Usando o exemplo sem fio acima, para uma organização selecionar "N/D" para os requisitos 1.2.3, 2.1.1 e 4.1.1, ela precisaria confirmar que não há tecnologias sem fio usadas em seu CDE ou que se conectem ao seu CDE. Após a confirmação, a organização deve selecionar "N/D" para esses requisitos específicos.

Se um requisito for completamente excluído da revisão sem quaisquer considerações de *aplicabilidade*, a opção "Não testado" deverá ser selecionada. Exemplos de situações nas quais isso poderia acontecer, incluem:

- O adquirente pode solicitar que uma organização valide um subconjunto de requisitos, por exemplo, usando uma abordagem priorizada para validar determinados eventos.
- Uma organização pode desejar validar um novo controle de segurança que impacte um subconjunto de requisitos, por exemplo, a implementação de uma nova metodologia de criptografia que exija a avaliação dos Requisitos 2, 3 e 4 do PCI DSS.
- Uma organização prestadora de serviços pode oferecer um serviço que abranja apenas um número limitado de requisitos de PCI DSS, por exemplo, um provedor de armazenamento físico pode apenas validar os controles de segurança física de acordo com o Requisito 9 do PCI DSS para sua instalação de armazenamento.

Nesses cenários, a organização pode validar determinados requisitos de PCI DSS, embora outros requisitos possam ser aplicáveis em seu ambiente.

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)		
☐ Varejo	☐ Telecomunicações	☐ Armazéns e Supermercados
☐ Petróleo	☐ Comércio eletrônico	☐ Pedido por correio/telefone (MOTO)
☐ Outros (especificar):		
Quais tipos de canais de pagamento seu negócio atende? ☐ Pedido por telefone/correio (MOTO) ☐ Comércio eletrônico ☐ Cartão presente (face a face)	Quais canais de pagamento são abrangidos por esse SAQ? ☐ Pedido por telefone/correio (MOTO) ☐ Comércio eletrônico ☐ 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 portador do cartão?	

Parte 2c. Locais

Listar os tipos de instalações (por exemplo, estabelecimentos comerciais, escritórios corporativos, data centers, centrais de atendimento etc.) e um resumo dos locais inclusos na revisão do PCI DSS.

Tipo de instalação	Número de instalações desse tipo	Local(is) da instalação (cidade, país)
Exemplo: Lojas de varejo	*3*	*Boston, MA, EUA*

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)
			☐Sim ☐ Não	
			☐Sim ☐ Não	
			☐Sim ☐ Não	
			☐Sim ☐ Não	
			☐Sim ☐ 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 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:**

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

Seção 2: Questionário de autoavaliação D para Comerciantes

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/A	Não testado
1.1	Os padrões de configuração do firewall e do roteador foram estabelecidos e implementados para incluir o seguinte:						
1.1.1	Existe um processo formal para aprovar e testar todas as conexões de rede e alterações nas configurações do firewall e do roteador?	▪ Reveja o processo documentado ▪ Entreviste a equipe ▪ Examine as configurações da rede	☐	☐	☐	☐	☐
1.1.2	(a) Há um diagrama de rede atual que identifica todas as conexões entre o ambiente dos dados do titular do cartão e outras redes, incluindo qualquer rede sem fio?	▪ Reveja o diagrama de rede atual ▪ Examine as configurações da rede	☐	☐	☐	☐	☐
	(b) Há um processo que garanta que o diagrama esteja atualizado?	▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
1.1.3	(a) Há um diagrama atual que mostra todos os fluxos de dados do portador do cartão pelos sistemas e redes?	▪ Reveja o diagrama atual de fluxo de dados ▪ Examine as configurações da rede	☐	☐	☐	☐	☐
	(b) Há um processo que garanta que o diagrama esteja atualizado?	▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
1.1.4	(a) Um firewall é exigido e implementado em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna?	▪ Reveja os padrões de configuração do firewall ▪ Observe as configurações de rede para verificar se o firewall está instalado	☐	☐	☐	☐	☐
	(b) O diagrama de rede atual está de acordo com os padrões de configuração do firewall?	▪ Compare os padrões de configuração do firewall com o diagrama de rede atual	☐	☐	☐	☐	☐
1.1.5	Os grupos, funções e responsabilidades para gerenciamento lógico dos componentes da rede são atribuídos e documentados nos padrões de configuração do roteador e do firewall?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Entreviste a equipe	☐	☐	☐	☐	☐
1.1.6	(a) Os padrões de configuração de firewall e roteador incluem uma lista documentada dos serviços, protocolos e portas, incluindo a justificativa e aprovação comercial para cada um?	▪ Reveja o firewall e os padrões de configuração do roteador	☐	☐	☐	☐	☐
	(b) Todos os serviços, protocolos e portas não seguros estão identificados e existem recursos de segurança documentados e implementados para cada um desses serviços identificados?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.1.7	(a) Os padrões de configuração do firewall e do roteador exigem a análise dos conjuntos de regras do firewall e do roteador pelo menos a cada seis meses?	▪ Reveja o firewall e os padrões de configuração do roteador	☐	☐	☐	☐	☐
	(b) Os conjuntos de regras do firewall e do roteador são analisados pelo menos a cada seis meses?	▪ Examine a documentação das análises do firewall	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
	(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)?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.2.2	Os arquivos de configuração do roteador estão seguros em relação ao acesso não autorizado e sincronizado—por exemplo, a configuração em execução (ou ativa) corresponde à configuração inicial (usada quando as máquinas são iniciadas)?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine os arquivos de configuração do roteador e as configurações do roteador	☐	☐	☐	☐	☐
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?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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:						
1.3.1	Existe uma DMZ implementada para limitar o tráfego de entrada somente para componentes do sistema que fornecem serviços, portas e protocolos autorizados acessíveis publicamente?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.3.2	O tráfego de internet de entrada está limitado ao endereço IP dentro da DMZ?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.3.3	As medidas contra falsificação estão implementadas para detectar e impedir que endereços IP de fonte falsificada entrem na rede? (Por exemplo, bloquear tráfego originado da internet com um endereço interno)	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.3.4	O tráfego de saída do ambiente de dados do titular do cartão para a internet está explicitamente autorizado?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.3.5	São permitidas apenas as conexões estabelecidas na rede?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
1.3.6	Os componentes do sistema que armazenam dados do titular do cartão (como banco de dados) estão localizados em uma zona da rede interna, separada da DMZ e de outras redes não confiáveis?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
1.3.7	(a) Existem métodos em vigor para evitar a divulgação de endereços IP privados e de informações de roteamento para a internet? ***Observação:*** *os métodos para ocultar o endereço IP podem incluir, entre outros:* • Conversão de endereços de rede (NAT) • Implementação dos servidores contendo dados do portador do cartão atrás dos servidores de proxy/firewalls, • Remoção ou filtragem das propagandas de rota para redes privadas que empregam endereçamento registrado, • Uso interno do espaço de endereço RFC1918 em vez de endereço registrado.	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐	☐
	(b) A divulgação dos endereços IP privados e das informações de roteamento para entidades externas é autorizada?	▪ Examine o firewall e as configurações do roteador ▪ Entreviste a equipe	☐	☐	☐	☐	☐
1.4	(a) Está instalado e ativo um software de firewall pessoal (ou funcionalidade equivalente) em qualquer dispositivo portátil (incluindo da empresa e/ou de propriedade dos funcionários) que se conectam à internet quando fora da rede (por exemplo, laptops usados pelos funcionários), e que também são usados para acessar o CDE?	▪ Reveja as políticas e padrões de configuração ▪ Examine os dispositivos móveis e/ou de propriedade do funcionário	☐	☐	☐	☐	☐
	(b) O software de firewall pessoal (ou funcionalidade equivalente) está configurado para definições de configuração específicas, funcionando ativamente e não alterável por usuários de dispositivos móveis e/ou de propriedade dos funcionários?	▪ Reveja as políticas e padrões de configuração ▪ Examine os dispositivos móveis e/ou de propriedade do funcionário	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
1.5	Os procedimentos operacionais e as políticas de segurança para gerenciar os firewalls são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
2.1	(a) Os valores-padrão entregues pelo fornecedor são sempre alterados antes de instalar um sistema na rede? *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).*	▪ Reveja as políticas e procedimentos ▪ Examine a documentação do fornecedor ▪ Observe as configurações do sistema e as definições da conta ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) As contas-padrão desnecessárias são removidas ou desativadas antes da instalação de um sistema na rede?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema e as definições da conta ▪ Entreviste a equipe	☐	☐	☐	☐	☐
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?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) As strings de comunidades de SNMP padrão dos dispositivos sem fio são alteradas na instalação?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Entreviste a equipe ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(c) As senhas/frases de senha padrão dos pontos de acesso são alteradas na instalação?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(d) O firmware dos dispositivos sem fio é atualizado para ser compatível com a criptografia robusta para autenticação e transmissão em redes sem fio?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(e) Os outros padrões relacionados à segurança do fornecedor de dispositivos sem fio são alterados, se aplicável?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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? *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).*	▪ Reveja os padrões de configuração do sistema ▪ Reveja os padrões de fortalecimento aceitos pelo setor ▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) Os padrões de configuração do sistema são atualizados quando novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.1?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(c) Os padrões de configuração do sistema são aplicados quando novos sistemas são configurados?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(d) Os padrões de configuração do sistema incluem todos os seguintes itens: • 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?	▪ Reveja os padrões de configuração do sistema	☐	☐	☐	☐	☐
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? *Por exemplo, servidores da Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.*	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(b) Se forem usadas tecnologias de virtualização, somente uma função principal está implementada por componente ou dispositivo do sistema virtual?	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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)?	▪ Reveja os padrões de configuração ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(b) Todos os protocolos, daemons ou serviços não seguros e ativados são justificados de acordo com os padrões de configuração documentados?	▪ Reveja os padrões de configuração ▪ Entreviste a equipe ▪ Examine as definições de configuração ▪ Compare serviços ativos etc. com justificativas documentadas	☐	☐	☐	☐	☐
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.*	▪ Reveja os padrões de configuração ▪ Examine as definições de configuração	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) As configurações comuns dos parâmetros de segurança estão incluídas nos padrões de configuração do sistema?	▪ Reveja os padrões de configuração do sistema	☐	☐	☐	☐	☐
	(c) As configurações dos parâmetros de segurança estão definidas corretamente nos componentes do sistema?	▪ Examine os componentes do sistema ▪ Examine as definições de parâmetro de segurança ▪ Compare as definições com os padrões de configuração do sistema	☐	☐	☐	☐	☐
2.2.5	(a) Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da web desnecessários foram removidas?	▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐	☐
	(b) As funções ativadas estão documentadas e oferecem suporte para uma configuração segura?	▪ Reveja a documentação ▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐	☐
	(c) Existem somente funcionalidades registradas presentes nos componentes do sistema?	▪ Reveja a documentação ▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐	☐
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***						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(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?	▪ Examine os componentes do sistema ▪ Examine as configurações do sistema ▪ Observe o logon de um administrador	☐	☐	☐	☐	☐
	(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?	▪ Examine os componentes do sistema ▪ Examine os serviços e arquivos	☐	☐	☐	☐	☐
	(c) O acesso do administrador às interfaces de gerenciamento baseadas na web é criptografado com uma criptografia robusta?	▪ Examine os componentes do sistema ▪ Observe o logon de um administrador	☐	☐	☐	☐	☐
	(d) Para a tecnologia em uso, a criptografia robusta é implementada de acordo com as melhores práticas do setor e/ou recomendações do fornecedor?	▪ Examine os componentes do sistema ▪ Reveja a documentação do fornecedor ▪ Entreviste a equipe	☐	☐	☐	☐	☐
2.4	(a) Um inventário é mantido para os componentes do sistema que estão dentro do escopo para PCI DSS, incluindo uma lista de componentes de hardware e software e uma descrição da função/uso de cada?	▪ Examine o inventário do sistema	☐	☐	☐	☐	☐
	(b) O inventário documentado é mantido atualizado?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
2.5	Os procedimentos operacionais e as políticas de segurança para gerenciamento dos padrões do fornecedor e outros parâmetros de segurança são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
2.6	*Esse requisito aplica-se apenas aos prestadores de serviços.*						

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/A	Não testado
3.1	As políticas, procedimentos e processos de retenção e eliminação de dados são implementados conforme segue:						
	(a) A quantidade de armazenamento e tempo de retenção de dados é limitada ao exigido para requisitos legais, regulamentares e/ou comerciais?	▪ Reveja as políticas e procedimentos de retenção e eliminação de dados ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) Existem processos definidos para excluir com segurança dados de titulares de cartão quando não forem mais necessários por razões legais, regulamentares e/ou comerciais?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine o mecanismo de exclusão	☐	☐	☐	☐	☐
	(c) Há requisitos de retenção específicos para dados do titular do cartão? *Por exemplo, os dados do titular do cartão precisam ser retidos por um período X pelos motivos comerciais Y.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine os requisitos de retenção	☐	☐	☐	☐	☐
	(d) Há processos trimestrais para identificar e excluir com segurança os dados do titular do cartão que excederem os requisitos de retenção definidos?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os processos de exclusão	☐	☐	☐	☐	☐
	(e) Todos os dados armazenados do titular do cartão cumprem os requisitos definidos na política de retenção de dados?	▪ Examine os arquivos e os registros do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.2	(a) *Esse procedimento de teste aplica-se apenas aos emissores.*						
	(b) *Esse procedimento de teste aplica-se apenas aos emissores.*						
	(c) Os dados de autenticação confidenciais são excluídos ou deixados irrecuperáveis ao se completar o processo de autorização?	▪ Reveja as políticas e procedimentos ▪ Examine as configurações do sistema ▪ Examine os processos de exclusão	☐	☐	☐	☐	☐
	(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	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? *Esses dados também são denominados como rastreamento completo, rastreamento, rastreamento 1, rastreamento 2 e dados da tarja magnética.* ***Observação:*** *no curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser mantidos:* • *O nome do titular do cartão* • *Número da conta primária (PAN)* • *Data de vencimento e* • *Código de serviço* *Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.*	▪ Examine as fontes de dados, incluindo: • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Examine as fontes de dados, incluindo: • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados	☐	☐	☐	☐	☐
3.2.3	Após a autorização, o número de identificação funcionários (PIN) ou o bloqueio de PIN criptografado não é armazenado?	▪ Examine as fontes de dados, incluindo: • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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 ? ***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).*	▪ 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	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	**Sim com CCW**	**Não**	**N/A**	**Não testado**
3.4	O PAN é processado para ficar ilegível em qualquer local onde ele esteja armazenado (incluindo repositórios de dados, mídias digitais portáteis, mídias de backup e logs de auditoria) usando qualquer uma das seguintes abordagens? ▪ Hash de direção única com base na criptografia forte (o hash deve ser do PAN inteiro) ▪ Truncamento (a codificação hash não pode ser usada para substituir o segmento truncado do PAN) ▪ Tokens e blocos de índice (os blocos devem ser armazenados de forma segura) ▪ Criptografia robusta com processos e procedimentos de gerenciamento-chave associados. ***Observação:*** *É um esforço relativamente simples para um indivíduo mal-intencionado reconstituir os dados do PAN original caso ele tenha acesso às versões truncadas e hash do PAN. Onde estiverem presentes versões obscurecidas e truncadas de mesmo PAN no ambiente da entidade, controles adicionais devem existir para garantir que as versões truncadas e obscurecidas não possam ser correlacionadas para reconstruir o PAN original.*	▪ Examine a documentação do fornecedor ▪ Examine os repositórios de dados ▪ Examine as mídias removíveis ▪ Examine os registros de auditoria, incluindo registros de aplicativo de pagamento	☐	☐	☐	☐	☐
3.4.1	Se a criptografia de disco (e não a criptografia do banco de dados no nível de coluna ou de arquivo) for utilizada, o acesso é gerenciado das formas a seguir? ***Observação:*** *Este requisito aplica-se também a todos os outros requisitos de gerenciamento de chaves e criptografia de PCI DSS*						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(a) O acesso lógico aos sistemas de arquivos criptografados é gerenciado de forma separada e independente dos mecanismos de controle de acesso e autenticação do sistema operacional nativo (por exemplo, não usando bancos de dados de conta de usuário local ou credenciais de logon de rede geral)?	▪ Examine as configurações do sistema ▪ Observe o processo de autenticação	☐	☐	☐	☐	☐
	(b) As chaves criptográficas são armazenadas de forma segura (por exemplo, armazenadas em mídias removíveis protegidas adequadamente com controles de acesso robustos)?	▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(c) Os dados do portador do cartão nas mídias removíveis estão criptografados onde quer que estejam armazenados? ***Observação:*** *se a criptografia de dados não for usada para criptografar a mídia removível, os dados armazenados nessa mídia deverão ser tornados ilegíveis por meio de outro método.*	▪ Examine as configurações do sistema ▪ Observe os processos	☐	☐	☐	☐	☐
3.5	Alguma chave é usada para proteger os dados do titular do cartão contra divulgação e uso inapropriado das formas a seguir: ***Observação:*** *esse requisito aplica-se a chaves usadas para criptografar os dados armazenados do portador do cartão, bem como as chaves de criptografia principais usadas para proteger as chaves de criptografia de dados. Essas chaves de criptografia de chaves devem ser tão robustas quanto a chave de criptografia de dados.*						
3.5.1	*Esse requisito aplica-se apenas a prestadores de serviços*						
3.5.2	O acesso às chaves criptográficas está restrito ao menor número necessário de responsáveis pela proteção?	▪ Examine as listas de acesso do usuário	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.5.3	As chaves de criptografia secretas e privadas são usadas para criptografar/descriptografar dados armazenados em uma (ou mais) das seguintes formas em todos os momentos? ▪ Criptografadas com uma chave de criptografia de chaves que seja ao menos tão forte quanto a chave de criptografia de dados e que esteja armazenada separadamente da chave de criptografia de dados. ▪ Dentro de um dispositivo criptográfico seguro (por exemplo, um módulo de segurança de hardware (host) (HSM) ou dispositivo de ponto-de-interação aprovado por PTS). ▪ Como pelo menos duas partes de chave ou componentes de chave de tamanho total, de acordo com um método aceito pelo setor. ***Observação:*** *não é exigido que chaves públicas sejam armazenadas em uma destas formas.*	▪ Reveja os procedimentos documentados ▪ Examine as configurações do sistema e os locais principais de armazenamento, incluindo as chaves de criptografia principais	☐	☐	☐	☐	☐
3.5.4	As chaves de criptografia são armazenadas no menor número possível de locais?	▪ Examine os locais de armazenamento das chaves ▪ Observe os processos	☐	☐	☐	☐	☐
3.6	(a) Todos os processos e procedimentos de gerenciamento de chaves das chaves criptográficas usadas para criptografar os dados do titular do cartão estão totalmente documentados e implementados?	▪ Reveja os procedimentos de gerenciamento das chaves	☐	☐	☐	☐	☐
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
	(c) Existem processos e procedimentos de gerenciamento de chaves implementados que requerem os itens a seguir?						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.6.1	Os procedimentos de chaves criptográficas incluem a geração de chaves criptográficas robustas?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Observe o método de geração de chave	☐	☐	☐	☐	☐
3.6.2	Os procedimentos de chaves criptográficas incluem a distribuição segura das chaves criptográficas?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Observar os procedimentos de distribuição de chave	☐	☐	☐	☐	☐
3.6.3	Os procedimentos de chaves criptográficas incluem o armazenamento seguro das chaves criptográficas?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Observe o método para armazenamento seguro das chaves	☐	☐	☐	☐	☐
3.6.4	Os procedimentos de chaves criptográficas incluem alterações das chaves criptográficas para chaves que alcançaram o final de seu período de criptografia (por exemplo: após um período de tempo definido e/ou após a produção de certa quantidade de texto criptografado por determinada chave), conforme definido pelo fornecedor associado do aplicativo ou pelo proprietário da chave, com base nas melhores práticas e orientações do setor (como a NIST Special Publication 800-57)?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.6.5	(a) Os procedimentos de chaves criptográficas incluem a inutilização ou substituição (por exemplo: por arquivamento, destruição e/ou revogação) das chaves criptográficas quando a integridade da chave estiver enfraquecida (como a saída de um funcionário com conhecimento de uma chave em texto simples)?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) Os procedimentos de chaves criptográficas incluem a substituição de chaves comprometidas conhecidas ou suspeitas?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(c) Se chaves criptografadas inutilizadas ou substituídas forem mantidas, elas são usadas somente para fins de decriptografia/verificação e não para criptografia?	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.6.6	Se as operações manuais de gerenciamento de chave em texto claro são usadas, os procedimentos de chave de criptografia incluem conhecimento separado e controle duplo das chaves de criptografia, conforme a seguir: ▪ O conhecimento separado exige que os componentes de chaves estejam sob o controle de pelo menos duas pessoas que têm conhecimento apenas de seus próprios componentes de chave? E ▪ Os procedimentos de controle duplo de chaves exigem pelo menos duas pessoas para executar qualquer operação de gerenciamento de chave e que uma única pessoa não tenha acesso aos materiais de autenticação (por exemplo, senhas ou chaves) do outro? ***Observação:*** *os exemplos de operações manuais de gerenciamento de chave incluem, entre outros, geração, transmissão, carregamento, armazenamento e destruição de chaves.*	▪ Reveja os procedimentos de gerenciamento das chaves ▪ Entreviste a equipe e/ou ▪ Observe os processos	☐	☐	☐	☐	☐
3.6.7	Os procedimentos de chaves criptográficas incluem a prevenção contra a substituição não autorizada de chaves criptográficas?	▪ Reveja os procedimentos ▪ Entreviste a equipe e/ou ▪ Observe os processos	☐	☐	☐	☐	☐
3.6.8	Os responsáveis pela proteção das chaves criptográficas devem reconhecer formalmente (por escrito ou eletronicamente) que compreendem e aceitam suas responsabilidades de proteção das chaves?	▪ Reveja os procedimentos ▪ Reveja a documentação e outras evidências	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
3.7	As políticas de segurança e procedimentos operacionais para proteção dos dados armazenados do titular do cartão estão/são: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
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.* *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).*	▪ 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	☐	☐	☐	☐	☐
	(b) São aceitas apenas chaves e/ou certificados confiáveis?	▪ Observe as transmissões de entrada e saída ▪ Examine as chaves e certificados	☐	☐	☐	☐	☐
	(c) São implementados protocolos de segurança para usar apenas configurações seguras e não apoiar versões ou configurações inseguras?	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(d) A força adequada da criptografia foi implementada para a metodologia de criptografia em uso (verifique as recomendações/melhores práticas do fornecedor)?	▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
	(e) Para implementações de TLS, o TLS é habilitado sempre que dados de titulares de cartão são transmitidos ou recebidos? *Por exemplo, para implementações com base no navegador:* • *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.	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Reveja os padrões documentados ▪ Reveja as redes sem fio ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
4.2	(a) Os PANs são processados de modo ilegível ou protegido com criptografia forte sempre que são enviados através das tecnologias de mensagens de usuário final (por exemplo, e-mail, mensagens instantâneas, SMS, chat, etc.)?	▪ Observe os processos ▪ Reveja as transmissões de saída	☐	☐	☐	☐	☐
	(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?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
4.3	As políticas de segurança e procedimentos operacionais para transmissão criptografada de dados do titular do cartão são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
5.1	Os softwares antivírus estão implementados em todos os sistemas normalmente afetados por softwares mal-intencionados?	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
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)?	▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐	☐
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?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
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?	▪ Examine as políticas e procedimentos ▪ Examine as configurações do antivírus, incluindo a instalação principal ▪ Examine os componentes do sistema	☐	☐	☐	☐	☐
	(b) As atualizações automáticas e as varreduras periódicas estão ativadas e sendo executadas?	▪ Examine as configurações do antivírus, incluindo a instalação principal ▪ Examine os componentes do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(c) Todos os mecanismos antivírus geram logs de auditoria e os logs são mantidos de acordo com o Requisito 10.7 do PCI DSS?	▪ Examine as configurações do antivírus ▪ Reveja os processos de retenção de registro	☐	☐	☐	☐	☐
5.3	Todos os mecanismos do antivírus: ▪ Estão sendo executados ativamente? ▪ Não podem ser desativados ou alterados pelos usuários? ***Observação:*** *as soluções de antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período de tempo durante o qual a proteção antivírus não estiver ativa.*	▪ Examine as configurações do antivírus ▪ Examine os componentes do sistema ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
5.4	Os procedimentos operacionais e as políticas de segurança para proteção dos sistemas contra malware são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
6.1	Há um processo para identificar vulnerabilidades de segurança, incluindo o seguinte: ▪ 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"? ***Observação**: as classificações de risco devem ser baseadas nas práticas recomendadas pelo setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.* *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.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
	(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.*	▪ 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	☐	☐	☐	☐	☐
6.3	(a) Os processos de desenvolvimento de software são baseados nos padrões e/ou melhores práticas do setor?	▪ Reveja os processos de desenvolvimento do software ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) A segurança das informações está incluída no ciclo de vida de desenvolvimento de softwares?	▪ Reveja os processos de desenvolvimento do software ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(c) Os aplicativos de software são desenvolvidos de acordo com o PCI DSS (com autenticação e logs seguros, por exemplo)?	▪ Reveja os processos de desenvolvimento do software ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(d) Os processos de desenvolvimento de softwares garantem o seguinte nos requisitos 6.3.1 - 6.3.2:						
6.3.1	As contas de desenvolvimento, teste e/ou aplicativos personalizados, IDs de usuário e senhas são removidas antes que o aplicativo se torne ativo ou seja lançado aos clientes?	▪ Reveja os processos de desenvolvimento do software ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	**Sim com CCW**	**Não**	**N/A**	**Não testado**
6.3.2	Os códigos personalizados são analisados antes da liberação para produção ou da distribuição aos clientes para identificar qualquer possível vulnerabilidade no código (usando processos manuais ou automatizados), conforme os itens a seguir: ▪ As alterações dos códigos são analisadas por outras pessoas além do autor do código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras? ▪ As revisões de código garantem que o código seja desenvolvido de acordo com as diretrizes de codificação seguras? ▪ As correções adequadas são implementadas antes da distribuição? ▪ Os resultados das análises dos códigos são revisados e aprovados pela gerência antes da distribuição? ***Observação**: Este requisito referente às análises dos códigos se aplica a todos os códigos personalizados (internos e voltados ao público), como parte integrante do ciclo de vida de desenvolvimento do sistema. As análises dos códigos podem ser realizadas por equipes internas instruídas ou terceiros. Os aplicativos da Web voltados ao público também estão sujeitos a controles extras para abranger ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.6 do PCI DSS.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine as alterações recentes e registros das alterações	☐	☐	☐	☐	☐
6.4	Os processos e procedimentos de controle de alterações foram seguidos para todas as alterações nos componentes do sistema para incluir os itens a seguir?						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
6.4.1	(a) Os ambientes de teste/desenvolvimento são separados do ambiente de produção?	▪ Reveja os procedimentos e processos de controle de alteração ▪ Examine a documentação de rede e as configurações do dispositivo de rede	☐	☐	☐	☐	☐
	(b) O controle de acesso usado força a separação dos ambientes de desenvolvimento/teste e o ambiente de produção?	▪ Reveja os procedimentos e processos de controle de alteração ▪ Examine as definições do controle de acesso	☐	☐	☐	☐	☐
6.4.2	Existe uma separação das tarefas entre a equipe atribuída aos ambientes de desenvolvimento/teste e a equipe atribuída ao ambiente de produção?	▪ Reveja os procedimentos e processos de controle de alteração ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
6.4.3	Os dados de produção (PANs ativos) ***não*** são usados para testes ou desenvolvimento?	▪ Reveja os procedimentos e processos de controle de alteração ▪ Observe os processos ▪ Entreviste a equipe ▪ Examine os dados de teste	☐	☐	☐	☐	☐
6.4.4	São removidos os dados de teste e contas dos componentes do sistema antes de o sistema se tornar ativo/entrar em produção?	▪ Reveja os procedimentos e processos de controle de alteração ▪ Observe os processos ▪ Entreviste a equipe ▪ Examine os sistemas de produção	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
6.4.5	(a) São documentados os procedimentos de controle de alterações e requerem o seguinte? • Documentação de impacto • Aprovação de controle de alteração documentada pelas partes autorizadas • Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema • Procedimentos de reversão	▪ Reveja os procedimentos e processos de controle de alteração	☐	☐	☐	☐	☐
	(b) Os seguintes itens são executados e documentados para todas as mudanças:						
6.4.5.1	Documentação de impacto?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐	☐
6.4.5.2	Aprovação documentada pelas partes autorizadas	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐	☐
6.4.5.3	(a) A funcionalidade é testada para verificar se a alteração não tem impacto adverso sobre a segurança do sistema?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐	☐
	(b) Para alterações do código personalizado, todas as atualizações foram testadas para conformidade com o Requisito 6.5 do PCI DSS antes de serem implantadas na produção?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
6.4.5.4	Procedimentos de back-out?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐	☐
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 é 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.*	▪ 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	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
6.5	(a) Os processos de desenvolvimento do software abordam vulnerabilidades de codificação comum?	▪ Reveja os procedimentos e políticas de desenvolvimento de software	☐	☐	☐	☐	☐
	(b) Os desenvolvedores são treinados pelo menos anualmente em técnicas de codificação seguras atualizadas, incluindo como evitar vulnerabilidades comuns de codificação?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Examine os registros de treinamento	☐	☐	☐	☐	☐
	(c) Os aplicativos são desenvolvidos com base nas diretrizes de codificação segura para proteger aplicativos das seguintes vulnerabilidades, no mínimo: ***Observação:*** *as vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas de acordo com as práticas recomendadas pelo setor, quando esta versão do PCI DSS foi publicada. No entanto, conforme as melhores práticas do setor para o gerenciamento de vulnerabilidades são atualizadas (por exemplo, o Guia Open Web Application Security Project (OWASP), SANS CWE Top 25, CERT Secure Coding, etc.), as melhores práticas atuais precisam ser usadas para estes requisitos.*						
6.5.1	As técnicas de codificação direcionam defeitos de injeção, particularmente injeção SQL? ***Observação:*** *também considere as falhas de injeção OS Command Injection, LDAP e XPath, assim como outras falhas.*	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.2	As técnicas de codificação direcionam as vulnerabilidades de estouro de buffer?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	**Sim com CCW**	**Não**	**N/A**	**Não testado**
6.5.3	As técnicas de codificação abordam o armazenamento criptográfico não seguro?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.4	As técnicas de codificação abordam as comunicações não seguras?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.5	As técnicas de codificação abordam a manipulação incorreta de erros?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.6	As técnicas de codificação abordam todas as vulnerabilidades classificadas como de "alto risco" identificadas no processo de identificação de vulnerabilidade (conforme definido no Requisito 6.1 do PCI DSS)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
Para as interfaces de aplicativo e aplicativos da Web (internos ou externos), os aplicativos são desenvolvidos com base nas diretrizes de codificação segura para proteger os aplicativos das seguintes vulnerabilidades adicionais:							
6.5.7	As técnicas de codificação direcionam as vulnerabilidades de script entre sites (XSS)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
6.5.8	As técnicas de controle direcionam controle inadequado de acesso, como referências diretas não seguras a objetos, falhas em restringir o acesso a URLs, diretórios transversais e falhas em restringir o acesso do usuário às funções?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.9	As técnicas de codificação direcionam falsificação de solicitação entre sites (CSRF)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
6.5.10	As técnicas de codificação direcionam gerenciamento de sessão e autenticação inválida?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

6.6	Para aplicativos da web voltados para o público, as novas ameaças e vulnerabilidades são abordadas continuamente, e esses aplicativos estão protegidos contra ataques conhecidos por *qualquer* um dos métodos a seguir? ▪ Analisando os aplicativos da web voltados para o público por meio de ferramentas ou métodos manuais ou automáticos de avaliação de segurança das vulnerabilidades dos aplicativos, conforme os itens a seguir: - Pelo menos uma vez ao ano - Após quaisquer alterações - Por meio de uma empresa especializada na segurança de aplicativos - Se, pelo menos, todas as vulnerabilidades no Requisito 6.5 estão incluídas na avaliação - Se todas as vulnerabilidades são corrigidas - Se o aplicativo for reavaliado após as correções ***Observação**: esta avaliação não é igual às varreduras de vulnerabilidades realizadas para o Requisito 11.2.* – **OU** – ▪ Instalar uma solução técnica automatizada que detecta e previne ataques baseados na web (por exemplo, um firewall de aplicativo da web) conforme a seguir: - Está situada diante de aplicativos da web voltados ao público para detectar e prevenir invasões baseadas na web. - Está funcionando ativamente e atualizada conforme aplicável. - Está gerando logs de auditoria. - Está configurado para bloquear ataques baseados na web, ou gerar um alerta que é imediatamente investigado.	▪ Reveja os processos documentados ▪ Entreviste a equipe ▪ Examine os registros de avaliações de segurança de aplicativo ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
6.7	Os procedimentos operacionais e as políticas de segurança para o desenvolvimento e manutenção dos aplicativos e sistemas seguros são/estão: ▪ Documentados ▪ Em uso	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	▪ Conhecidos por todas as partes envolvidas						

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/A	Não testado
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:						
	▪ Há uma política escrita para o controle de acesso que incorpore o seguinte? • Definir necessidades de acesso e atribuições especiais para cada função • Restrição de acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função, • A concessão do acesso se baseia na classificação e na atribuição da função da equipe individual • Aprovação documentada (eletronicamente ou por escrito) pelas partes autorizadas a todo o acesso, incluindo lista de privilégios específicos aprovados	▪ Examine a política escrita de controle de acesso	☐	☐	☐	☐	☐
7.1.1	Há necessidades de acesso para cada função, incluindo: ▪ Componentes do sistema e recursos de dados que cada função precisa acessar para realizar seu trabalho? ▪ O nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar os recursos.	▪ Examine as funções e necessidades de acesso	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
7.1.2	O acesso aos IDs de usuários privilegiados é restrito ao seguinte: ▪ Restrito ao menor número de privilégios necessários para o desempenho das responsabilidades da função? ▪ Permitido apenas às funções que requerem especificamente tal acesso privilegiado?	▪ Entreviste a equipe ▪ Entreviste os gerentes ▪ Reveja os IDs de usuários privilegiados	☐	☐	☐	☐	☐
7.1.3	O acesso é baseado na classificação e na atribuição individual da função da equipe?	▪ Entreviste os gerentes ▪ Reveja os IDs dos usuários	☐	☐	☐	☐	☐
7.1.4	Há uma aprovação documentada por partes autorizadas especificando os privilégios exigidos?	▪ Reveja os IDs dos usuários ▪ Compare com as aprovações documentadas ▪ Compare os privilégios atribuídos com as aprovações documentadas	☐	☐	☐	☐	☐
7.2	Existe um sistema de controle de acesso para componentes do sistema restringirem o acesso baseado na necessidade do usuário em conhecer, e está definido para "recusar todos" a menos que especificamente permitido, conforme a seguir?						
7.2.1	Existem sistemas de controle de acesso em todos os componentes do sistema?	▪ Reveja a documentação do fornecedor ▪ Examine as definições de configuração	☐	☐	☐	☐	☐
7.2.2	Os sistemas de controle de acesso são configurados para impor privilégios atribuídos aos indivíduos com base na classificação e função do trabalho?	▪ Reveja a documentação do fornecedor ▪ Examine as definições de configuração	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
7.2.3	Os sistemas de controle de acesso têm uma configuração padrão para "recusar todos"?	▪ Reveja a documentação do fornecedor ▪ Examine as definições de configuração	☐	☐	☐	☐	☐
7.3	Os procedimentos operacionais e políticas de segurança para a restrição de acesso aos dados do titular do cartão são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Examine as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
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, conforme a seguir:						
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?	▪ Reveja os procedimentos de senha ▪ Entreviste a equipe	☐	☐	☐	☐	☐
8.1.2	As adições, exclusões e modificações dos IDs, das credenciais e de outros objetos de identificação dos usuários são controladas de forma que os IDs dos usuários sejam implementados somente quando autorizados (incluindo usuários com privilégios específicos)?	▪ Reveja os procedimentos de senha ▪ Examine os IDs do usuário geral e privilegiado e as autorizações associadas ▪ Observe as definições do sistema	☐	☐	☐	☐	☐
8.1.3	O acesso dos usuários desligados da empresa é imediatamente desativado ou removido?	▪ Reveja os procedimentos de senha ▪ Examine as contas finalizadas de usuários ▪ Reveja as listas atuais de acesso ▪ Observe os dispositivos retornados de autenticação física	☐	☐	☐	☐	☐
8.1.4	As contas de usuários inativos são removidas ou desabilitadas no prazo de 90 dias?	▪ Reveja os procedimentos de senha ▪ Observe as contas do usuário	☐	☐	☐	☐	☐
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?	▪ Reveja os procedimentos de senha ▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) As contas de acesso remoto de terceiros são monitoradas quando em uso?	▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐	☐
8.1.6	(a) Tentativas repetidas de acesso estão limitadas ao bloquear o ID do usuário após seis tentativas, no máximo?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
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?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
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?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
8.2	Além de atribuir um ID exclusivo, um ou mais dos seguintes métodos foi empregado para autenticar todos os usuários? ▪ 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	▪ Reveja os procedimentos de senha ▪ Observe os processos de autenticação	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
8.2.1	(a) É usada uma criptografia forte para processar todas as credenciais de autenticação (como senhas/frases secretas) de modo ilegível durante o transporte e armazenamento em todos os componentes do sistema?	▪ Reveja os procedimentos de senha ▪ Reveja a documentação do fornecedor ▪ Examine as definições de configuração do sistema ▪ Observe os arquivos de senha ▪ Observe as transmissões de dados	☐	☐	☐	☐	☐
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
8.2.2	A identidade do usuário é identificada antes de se modificar qualquer credencial de autenticação, por exemplo, executar restauração da senha, provisionar novos tokens ou gerar novas chaves?	▪ Reveja os procedimentos de autenticação ▪ Observe a equipe	☐	☐	☐	☐	☐
8.2.3	(a) Os parâmetros de senha do usuário são configurados para exigir que as senhas/frases de senha atendam ao seguinte? • Exigir um tamanho mínimo de senha de pelo menos sete caracteres • Conter caracteres numéricos e alfabéticos Alternativamente, as senhas/frases secretas devem ter complexidade e força pelo menos equivalentes aos parâmetros especificados acima.	▪ Examine as definições da configuração do sistema para verificar os parâmetros de senha	☐	☐	☐	☐	☐
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
8.2.4	(a) As senhas de usuário/frases secretas são alteradas pelo menos uma vez a cada 90 dias?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
8.2.5	(a) Um indivíduo deve criar uma nova senha/frase secreta diferente das últimas quatro senhas/frases de senha usadas?	▪ Reveja os procedimentos de senha ▪ Amostra de componentes do sistema ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
	(b) *Esse procedimento de teste aplica-se apenas aos prestadores de serviços.*						
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?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema ▪ Observe a equipe de segurança	☐	☐	☐	☐	☐
8.3	Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE são protegidos usando-se a autenticação multifatores conforme a seguir? ***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 como autenticação multifatorial.*							

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
8.3.1	É incorporada autenticação multifatores para todos os acessos que não utilizam console no CDE para os funcionários com acesso administrativo? ***Observação:*** *Este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.*	▪ Examine as configurações do sistema ▪ Observar o login de administrador no CDE	☐	☐	☐	☐	☐
8.3.2	É incorporada autenticação multifatores em 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?	▪ Examine as configurações do sistema ▪ Observar os funcionários se conectando remotamente	☐	☐	☐	☐	☐
8.4	(a) Os procedimentos e políticas de autenticação são documentados e comunicados a todos os usuários?	▪ Reveja as políticas e procedimentos ▪ Reveja o método de distribuição ▪ Entreviste a equipe ▪ Entreviste os usuários	☐	☐	☐	☐	☐
	(b) Os procedimentos e políticas de autenticação incluem o seguinte? • 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	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação fornecida aos usuários	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
8.5	As contas e senhas (ou outros métodos de autenticação) de grupo, compartilhadas ou genéricas, são proibidas conforme os itens a seguir: • 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?	▪ Reveja as políticas e procedimentos ▪ Examine as listas de ID do usuário ▪ Entreviste a equipe	☐	☐	☐	☐	☐
8.5.1	*Esse requisito aplica-se apenas aos prestadores de serviços.*						
8.6	Onde forem usados outros mecanismos de autenticação (por exemplo, tokens de segurança físicos ou lógicos, cartões inteligentes, certificados, etc.), o uso destes mecanismos é atribuído como segue? • Os mecanismos de autenticação devem ser atribuídos a uma conta individual e não compartilhados entre várias contas • Controles físicos e/ou lógicos devem ser implementados para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine as definições da configuração do sistema e/ou controles físicos	☐	☐	☐	☐	☐
8.7	Todos os acessos para qualquer banco de dados que contenha dados do titular do cartão (incluindo acesso por meio de aplicativos, administradores e todos os outros usuários) são restritos conforme segue?						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(a) Todos os acessos, consultas e ações dos usuários (como transferências, cópias ou exclusões) nos bancos de dados são feitos somente por meio de métodos programáticos (como por meio dos procedimentos armazenados)?	▪ Reveja os procedimentos e políticas de autenticação de banco de dados ▪ Examine as definições de configuração de aplicativos e banco de dados	☐	☐	☐	☐	☐
	(b) O acesso direto ao usuário ou às consultas aos bancos de dados são restritas aos administradores do banco de dados?	▪ Reveja os procedimentos e políticas de autenticação de banco de dados ▪ Examine as definições do controle de acesso ao banco de dados ▪ Examine as definições de configuração de aplicativos de banco de dados	☐	☐	☐	☐	☐
	(c) Os IDs dos aplicativos só podem ser usados por aplicativos (e não por usuários individuais ou outros processos)?	▪ Reveja os procedimentos e políticas de autenticação de banco de dados ▪ Examine as definições do controle de acesso ao banco de dados ▪ Examine as definições de configuração de aplicativos de banco de dados	☐	☐	☐	☐	☐
8.8	Os procedimentos operacionais e políticas de segurança para a identificação e autenticação são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Examine as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A**	**Não testado**
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?	▪ Observe os controles de acesso físico ▪ Observe a equipe	☐	☐	☐	☐	☐
9.1.1	(a) Existem câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual em áreas sensíveis? ***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.*	▪ Reveja as políticas e procedimentos ▪ Observe os mecanismos de monitoramento físico ▪ Observe os recursos de segurança	☐	☐	☐	☐	☐
	(b) As câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) são protegidos contra adulteração ou desabilitação?	▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(c) São coletados dados das câmeras de vídeo e/ou mecanismos de controle de acesso vistos e correlacionados a outras entradas?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe de segurança	☐	☐	☐	☐	☐
	(d) Os dados das câmeras de vídeo e/ou dos mecanismos de controle de acesso são armazenados por pelo menos três meses, a menos que restrito por lei?	▪ Reveja os processos de retenção de dados ▪ Observe o armazenamento de dados ▪ Entreviste a equipe de segurança	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.1.2	Os controles físicos e/ou lógicos são usados para restringir o acesso a pontos de rede acessíveis publicamente? *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.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os locais	☐	☐	☐	☐	☐
9.1.3	O acesso físico aos pontos de acesso sem fio, gateways, dispositivos portáteis, hardwares de comunicação/rede e linhas de telecomunicação é restrito?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os dispositivos	☐	☐	☐	☐	☐
9.2	(a) Existem procedimentos desenvolvidos para diferenciar facilmente a equipe interna e os visitantes, conforme os itens a seguir: • Identificação de funcionários e de visitantes no local (por exemplo, crachás de identificação), • Modificar os requisitos de acesso e • Anular identificações de funcionários que se desligaram da empresa e de visitantes que encerraram sua atividade (como crachás de identificação) *Para as finalidades do Requisito 9, "equipe interna" refere-se a funcionários que trabalham em período integral e meio-período e funcionários, prestadores de serviços e consultores temporários que estão fisicamente presentes no endereço da entidade. Um "visitante" refere-se a um fornecedor, convidado de um funcionário, equipes de serviço ou qualquer pessoa que precise adentrar as dependências por um breve período, normalmente um dia, no máximo.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os métodos de identificação (por exemplo, crachás) ▪ Observe os processos do visitante	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) Os métodos de identificação (por exemplo, crachás) identificam claramente os visitantes e diferenciam facilmente os visitantes dos membros da equipe interna?	▪ Observe os métodos de identificação	☐	☐	☐	☐	☐
	(c) O acesso ao sistema de crachás é limitado aos funcionários autorizados?	▪ Observe os controles de acesso e controles físicos para o sistema de crachá	☐	☐	☐	☐	☐
9.3	O acesso físico dos funcionários às áreas confidenciais é controlado conforme segue: ▪ O acesso é autorizado e baseado na função do indivíduo? ▪ O acesso é revogado imediatamente após o término da atividade? ▪ Após o término da atividade, todos os mecanismos de acesso físico, como chaves, cartões de acesso, etc., são devolvidos e desativados?	▪ Entreviste a equipe ▪ Examine as listas de controle de acesso ▪ Observe a equipe interna ▪ Compare as listas de ex-funcionários com as listas de controle de acesso	☐	☐	☐	☐	☐
9.4	A identificação e o acesso do visitante são tratados como segue:						
9.4.1	Os visitantes são autorizados antes de entrar e sempre estão acompanhados em áreas nas quais os dados do titular do cartão são processados ou mantidos?	▪ Reveja as políticas e procedimentos ▪ Observe os processos do visitante, incluindo como o acesso é controlado ▪ Entreviste a equipe ▪ Observe os visitantes e o uso do crachá	☐	☐	☐	☐	☐
9.4.2	(a) Os visitantes são identificados e recebem um crachá ou outra identificação que distingue visivelmente os visitantes dos funcionários internos?	▪ Observe o uso do crachá dos funcionários e dos visitantes ▪ Examine a identificação	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) Os crachás ou outra identificação dos visitantes expiram?	▪ Observe o processo ▪ Examine a identificação	☐	☐	☐	☐	☐
9.4.3	É solicitado que os visitantes apresentem o crachá ou identificação antes de sair das dependências ou na data do vencimento?	▪ Observe os processos ▪ Observe a saída dos visitantes da instalação	☐	☐	☐	☐	☐
9.4.4	(a) Existe um log de visitantes em vigor para registrar o acesso físico às dependências, assim como aos ambientes com computador e centrais de dados onde os dados do titular do cartão são armazenados ou transmitidos?	▪ Reveja as políticas e procedimentos ▪ Examine o registro do visitante ▪ Observe os processos do visitante ▪ Examine a retenção do registro	☐	☐	☐	☐	☐
	(b) O registro contém o nome do visitante, a empresa representada e o funcionário interno que autoriza o acesso físico?	▪ Reveja as políticas e procedimentos ▪ Examine o registro do visitante	☐	☐	☐	☐	☐
	(c) O registro do visitante é mantido por pelo menos três meses?	▪ Reveja as políticas e procedimentos ▪ Examine a retenção do registro do visitante	☐	☐	☐	☐	☐
9.5	Todas as mídias estão fisicamente seguras (incluindo, entre outros, computadores, mídias eletrônicas removíveis, recibos em papel, relatórios em papel e faxes)? *Para os fins do requisito 9, "mídia" refere-se a todas as mídias em papel ou eletrônicas que contêm dados do titular do cartão.*	▪ Reveja as políticas e procedimentos para segurança física das mídias ▪ Entreviste a equipe	☐	☐	☐	☐	☐
9.5.1	O local onde os back-ups de mídia são armazenados são revisados pelo menos anualmente para confirmar que o armazenamento é seguro?	▪ Reveja as políticas e procedimentos para a análise dos locais de mídia externos ▪ Entreviste a equipe de segurança	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.6	(a) É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia?	▪ Reveja as políticas e procedimentos para distribuição de mídia	☐	☐	☐	☐	☐
	(b) Os controles incluem o seguinte:						
9.6.1	A mídia é classificada para que a confidencialidade dos dados possa ser determinada?	▪ Reveja as políticas e procedimentos para classificação de mídia ▪ Entreviste a equipe de segurança	☐	☐	☐	☐	☐
9.6.2	A mídia é enviada via um mensageiro seguro ou outro método de entrega que possa ser rastreado com precisão?	▪ Entreviste a equipe ▪ Examine a documentação e registros de rastreamento da distribuição de mídia	☐	☐	☐	☐	☐
9.6.3	A aprovação gerencial é obtida antes de mover as mídias (especialmente quando a mídia é distribuída a pessoas)?	▪ Entreviste a equipe ▪ Examine a documentação e registros de rastreamento da distribuição de mídia	☐	☐	☐	☐	☐
9.7	É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
9.7.1	(a) Os logs de inventário de todas as mídias recebem manutenção adequada?	▪ Examine os registros de inventário	☐	☐	☐	☐	☐
	(b) Os inventários periódicos de mídia são conduzidos pelo menos anualmente?	▪ Examine os registros de inventário ▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.8	(a) Todas as mídias são destruídas quando não são mais necessárias por razões corporativas ou legais?	▪ Reveja os procedimentos e políticas de destruição periódica de mídias	☐	☐	☐	☐	☐
	(b) Há uma política de destruição periódica das mídias que define os requisitos a seguir? • Materiais impressos devem ser triturados, incinerados ou amassados de forma que haja uma garantia razoável de que esses materiais não possam ser recuperados. • Os contêineres de armazenamento usados para os materiais a serem destruídos devem estar seguros. • Os dados dos titulares de cartão na mídia eletrônica devem ser processados de modo irrecuperável (por exemplo, através de um programa de limpeza segura em conformidade com os padrões aceitos da indústria para exclusão segura, ou destruindo fisicamente a mídia).	▪ Reveja os procedimentos e políticas de destruição periódica de mídias	☐	☐	☐	☐	☐
	(c) A destruição de mídias é executada da seguinte forma:						
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?	▪ Entreviste a equipe ▪ Examine os procedimentos ▪ Observe os processos	☐	☐	☐	☐	☐
	(b) Os contêineres usados para materiais que armazenam informações são destruídos de forma segura para prevenir o acesso aos conteúdos?	▪ Examine a segurança dos contêineres de armazenamento	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.8.2	Os dados do titular do cartão são processados na mídia eletrônica de modo irrecuperável (por exemplo, através de um programa de limpeza segura em conformidade com os padrões aceitos na indústria para exclusão segura, ou então destruindo fisicamente a mídia), de modo que os dados do titular do cartão não possam ser reconstruídos?	▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
9.9	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 conforme a seguir? ***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.*						
	(a) As políticas e procedimentos exigem que uma lista de tais dispositivos seja mantida?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
	(b) As políticas e procedimentos exigem que os dispositivos sejam periodicamente inspecionados quanto à falsificação ou substituição?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
	(c) As políticas e procedimentos exigem que os funcionários sejam treinados para reconhecer os comportamentos suspeitos e reportar a falsificação ou substituição de dispositivos?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.9.1	(a) A lista de dispositivos inclui o seguinte? • 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	▪ Examine a lista de dispositivos	☐	☐	☐	☐	☐
	(b) Essa lista é precisa e está atualizada?	▪ Observar os dispositivos e locais de dispositivos e comparar a lista	☐	☐	☐	☐	☐
	(c) Essa lista de dispositivos é atualizada quando dispositivos são adicionados, realocados, retirados de serviço etc?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
9.9.2	(a) As superfícies dos dispositivos são inspecionadas periodicamente para detectar falsificação (por exemplo, adição de espiões 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? ***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.*	▪ Entreviste a equipe ▪ Observe os processos de inspeção e compare-os com os processos definidos	☐	☐	☐	☐	☐
	(b) Os funcionários estão cientes dos procedimentos de inspeção dos dispositivos?	▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
9.9.3	Os funcionários são treinados para reconhecer tentativas de falsificação ou substituição de dispositivos para incluir o seguinte?						
	(a) Os materiais de treinamento para os funcionários nos locais dos pontos de venda incluem o seguinte? • 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).	▪ Reveja os materiais de treinamento	☐	☐	☐	☐	☐
	(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?	▪ Entrevista as equipes nos locais de POS	☐	☐	☐	☐	☐
9.10	Os procedimentos operacionais e políticas de segurança para a restrição de acesso físico aos dados do titular do cartão são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Examine as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
10.1	(a) Trilhas de auditoria estão habilitadas e ativas para os componentes do sistema?	▪ Observe os processos ▪ Entreviste o administrador do sistema	☐	☐	☐	☐	☐
	(b) O acesso aos componentes do sistema está ligado aos usuários individuais?	▪ Observe os processos ▪ Entreviste o administrador do sistema	☐	☐	☐	☐	☐
10.2	Foram implementadas trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:						
10.2.1	Todos os acessos individuais dos usuários aos dados do titular do cartão?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.2.2	Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.2.3	Acesso a todas as trilhas de auditoria?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.2.4	Tentativas inválidas de acesso lógico?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.2.6	Inicialização, interrupção ou pausa dos registros de auditoria?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.2.7	Criação e exclusão de objetos em nível de sistema?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
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?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.3.2	Tipo de evento?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.3.3	Data e hora?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
10.3.4	Indicação de sucesso ou falha?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.3.5	Origem do evento?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.3.6	Identidade ou nome dos dados, componentes do sistema ou recursos afetados?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐	☐
10.4	Todos os relógios e horários dos sistemas críticos estão sincronizados por meio do uso de uma tecnologia de sincronização e essa tecnologia é mantida atualizada? ***Observação:*** *um exemplo de tecnologia de sincronização de horários é o Network Time Protocol (NTP).*	▪ Reveja os processos e padrões de configuração de horário	☐	☐	☐	☐	☐
10.4.1	Os seguintes processos são implementados nos sistemas críticos para obter um horário consistente e correto:						
	(a) Apenas os servidores centrais de horário designados recebem sinais de horário de fontes externas e os sinais de horário de fontes externas são baseados no Tempo Atômico Internacional ou UTC?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) Onde houver mais de um servidor de horário designado, os servidores de horários se igualam um com o outro para manter a hora exata?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐	☐
	(c) Os sistemas recebem o horário somente dos servidores centrais de horário designados?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐	☐
10.4.2	Os dados de horário são protegidos conforme a descrição a seguir? (a) O acesso aos dados de horário é restrito somente às equipes com necessidades profissionais?	▪ Examine as configurações do sistema e as definições de sincronização de horário	☐	☐	☐	☐	☐
	(b) As alterações nas configurações de horários dos sistemas críticos são registradas, monitoradas e analisadas?	▪ Examine as configurações do sistema e os registros e configurações de sincronização de horário	☐	☐	☐	☐	☐
10.4.3	As configurações de horário são recebidas de fontes de horário específicas aceitas pelo setor (isso é feito para evitar a alteração do relógio por um indivíduo mal-intencionado)? *Além disso, essas atualizações podem ser criptografadas com uma chave simétrica e as listas de controle de acesso podem ser criadas para especificar os endereços IP das máquinas clientes que serão fornecidas com as atualizações de horário (para evitar o uso não autorizado de servidores de horário internos).*	▪ Examine as configurações do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
10.5	As trilhas de auditoria estão protegidas de forma que não possam ser alteradas, conforme a descrição a seguir?						
10.5.1	A visualização das trilhas de auditoria é limitada às pessoas com necessidades relacionadas à função?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐	☐
10.5.2	Os arquivos de trilha de auditoria estão protegidos contra modificações não autorizadas por meio de mecanismos de controle de acesso, separação física e/ou separação da rede?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐	☐
10.5.3	O backup dos arquivos de trilha de auditoria é feito imediatamente em um servidor de log centralizado ou em uma mídia que seja difícil de alterar?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐	☐
10.5.4	Os logs para tecnologias externas (por exemplo, sem fio, firewalls, DNS, e-mail) são escritos em um servidor ou mídia de registro interno, centralizado e seguro?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐	☐
10.5.5	São usados softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos logs para assegurar que os dados existentes do log não possam ser alterados sem gerar alertas (embora os novos dados que estejam sendo adicionados não gerem um alerta)?	▪ Examine as definições, arquivos monitorados e resultados das atividades de monitoramento	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
10.6	Os logs e ocorrências de segurança para todos os componentes do sistema são revisados para identificar irregularidades ou atividades suspeitas conforme a seguir? ***Observação:*** *as ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6*						
10.6.1	(a) Os procedimentos e políticas são definidos para analisar os seguintes itens ao menos diariamente, de modo manual ou por ferramentas de registro? • 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.)	▪ Reveja os procedimentos e políticas de segurança	☐	☐	☐	☐	☐
	(b) Os eventos de segurança e registros são analisados ao menos diariamente?	▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
10.6.2	(a) As políticas e os procedimentos de segurança são definidos para analisar os registros de todos os outros componentes do sistema periodicamente, seja de forma manual ou por meio de ferramentas de registros, com base nas políticas e na estratégia de gerenciamento de risco da organização?	▪ Reveja os procedimentos e políticas de segurança	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) Análises de todos os outros componentes do sistema são executadas de acordo com a política e a estratégia de gerenciamento de risco da organização?	▪ Reveja a documentação de avaliação de risco ▪ Entreviste a equipe	☐	☐	☐	☐	☐
10.6.3	(a) Os procedimentos e políticas escritos são definidos para acompanhar as exceções e anomalias identificadas durante o processo de análise?	▪ Reveja os procedimentos e políticas de segurança	☐	☐	☐	☐	☐
	(b) É executado um acompanhamento das exceções e anomalias?	▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐	☐
10.7	(a) Os procedimentos e políticas de retenção de log de auditoria estão sendo usados e exigem que os logs sejam mantidos por pelo menos um ano, com um mínimo de três meses de disponibilidade imediata de análise (por exemplo, online, arquivada ou restaurável por backup)?	▪ Reveja os procedimentos e políticas de segurança	☐	☐	☐	☐	☐
	(b) Os logs de auditoria são retidos pelo menos uma vez ao ano?	▪ Entreviste a equipe ▪ Examine os logs de auditoria	☐	☐	☐	☐	☐
	(c) Ao menos os últimos três meses de logs estão imediatamente disponíveis para análise?	▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐	☐
10.8	*Esse requisito aplica-se apenas a prestadores de serviços*						
10.9	Os procedimentos operacionais e políticas de segurança para o monitoramento de todo o acesso aos dados do titular do cartão e recursos da rede são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
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.*	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
	(b) A metodologia detecta e identifica qualquer ponto de acesso sem fio não autorizado, incluindo ao menos os itens a seguir? • 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.	▪ Avalie a metodologia	☐	☐	☐	☐	☐
	(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?	▪ Examine o resultado das varreduras sem fio recentes	☐	☐	☐	☐	☐
	(d) Se o monitoramento automatizado for utilizado (como IDS/IPS sem fio, NAC, etc.), ele está configurado para gerar alertas à equipe?	▪ Examine as definições de configuração	☐	☐	☐	☐	☐
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?	▪ Examine os registros do inventário	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Examine o plano de resposta a incidentes (veja o Requerimento 12.10)	☐	☐	☐	☐	☐
	(b) São tomadas ações quando os pontos de acesso sem fio não autorizados são encontrados?	▪ Entreviste a equipe responsável ▪ Inspecione as varreduras sem fio recentes e as respostas relacionadas	☐	☐	☐	☐	☐
11.2	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? ***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.* *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.*						
11.2.1	(a) As varreduras das vulnerabilidades internas são executadas trimestralmente?	▪ Reveja os relatórios de varredura	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(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?	▪ Reveja os relatórios de varredura	☐	☐	☐	☐	☐
	(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)?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
11.2.2	(a) As varreduras das vulnerabilidades externas são executadas trimestralmente? ***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.*	▪ Reveja os resultados dos quatro últimos trimestres quanto às varreduras de vulnerabilidades externas	☐	☐	☐	☐	☐
	(b) Os resultados da varredura externa trimestral cumprem os requisitos do *Guia do programa ASV* (por exemplo, nenhuma vulnerabilidade classificada com valor 4 ou superior pelo CVSS e nenhuma falha automática)?	▪ Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente	☐	☐	☐	☐	☐
	(c) As varreduras de vulnerabilidades externas trimestrais são executadas por um fornecedor de varredura aprovado (ASV) pela PCI SSC?	▪ Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente	☐	☐	☐	☐	☐
11.2.3	(a) Varreduras internas e externas e novas varreduras são realizadas, se necessário, após qualquer mudança significativa? ***Observação:*** *As varreduras devem ser realizadas por uma equipe qualificada.*	▪ Examine e correlacione a documentação de controle de alteração e os relatórios de varredura	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) O processo de varredura inclui novas varreduras até que: • 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)?	▪ Reveja os relatórios de varredura	☐	☐	☐	☐	☐
	(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)?	▪ Entreviste a equipe	☐	☐	☐	☐	☐
11.3	A metodologia de teste de penetração inclui o seguinte? ▪ É baseada nas abordagens de testes de penetração aceitas pelo setor (por exemplo, NIST SP800-115) ▪ Abrange todo o perímetro do CDE e sistemas críticos ▪ Inclui testes de dentro e fora da rede ▪ Inclui testes para validar qualquer controle de redução no escopo e segmentação ▪ Define testes de penetração da camada do aplicativo para incluir, pelo menos, as vulnerabilidades listadas no requisito 6.5 ▪ Define testes de penetração da camada da rede que incluam componentes compatíveis com as funções da rede e com os sistemas operacionais ▪ Inclui revisão e consideração de ameaças e vulnerabilidades ocorridas nos últimos 12 meses ▪ Especifica a retenção dos resultados de testes de penetração e resultados de atividades de reparo	▪ Examine a metodologia de teste de penetração ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
11.3.1	(a) É realizado um teste de penetração *externo* pela metodologia definida, pelo menos anualmente e após qualquer alteração significativa de infraestrutura ou aplicativo no ambiente (como uma atualização do sistema operacional, uma adição de subrede no ambiente, ou um servidor da web adicionado)?	▪ Examine o escopo do trabalho ▪ Examine os resultados do teste mais recente de penetração externa	☐	☐	☐	☐	☐
	(b) São realizados testes por um recurso interno qualificado ou terceiro externo qualificado e, se for o caso, existe a independência organizacional do testador (não é requerido ser um QSA ou ASV)?	▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
11.3.2	(a) É realizado um *teste de penetração interna pela metodologia definida, pelo menos anualmente e após qualquer mudança significativa de infraestrutura ou de aplicativo no ambiente (como uma atualização de sistema operacional, uma subrede adicionada ao ambiente, ou um servidor da web adicionado)?*	▪ Examine o escopo do trabalho ▪ Examine os resultados do teste mais recente de penetração interna	☐	☐	☐	☐	☐
	(b) São realizados testes por um recurso interno qualificado ou terceiro externo qualificado e, se for o caso, existe a independência organizacional do testador (não é requerido ser um QSA ou ASV)?	▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
11.3.3	As vulnerabilidades exploráveis encontradas durante o teste de penetração são corrigidas e o teste é repetido para verificar as correções?	▪ Examine os resultados do teste de penetração	☐	☐	☐	☐	☐
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?	▪ Examine os controles de segmentação ▪ Reveja a metodologia de teste de penetração	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(b) O teste de penetração para verificar os controles de segmentação atende ao seguinte? • 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	▪ Examine os resultados do teste mais recente de penetração	☐	☐	☐	☐	☐
	(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)?	▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
11.3.4.1	*Esse requisito aplica-se apenas a prestadores de serviços*						
11.4	(a) As técnicas de prevenção contra intrusão e/ou detecção de intrusão que detectam e/ou evitam instruções na rede estão em uso para monitorar todo o tráfego: • No perímetro do ambiente dos dados do titular do cartão, e • Nos pontos críticos do ambiente dos dados do titular do cartão.	▪ Examine as configurações do sistema ▪ Examine os diagramas da rede	☐	☐	☐	☐	☐
	(b) As técnicas de prevenção contra intrusão e/ou detecção de intrusão estão configuradas para alertar a equipe sobre comprometimentos suspeitos?	▪ Examine as configurações do sistema ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
	(c) Todos os mecanismos, diretrizes e assinaturas para detecção e prevenção contra invasões estão atualizados?	▪ Examine as configurações de IDS/IPS ▪ Examine a documentação do fornecedor	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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? *Os exemplos de arquivos que devem ser monitorados incluem:* • *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)*	▪ Observe as definições do sistema e os arquivos monitorados ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
	(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? ***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).*	▪ Observe as definições do sistema e os arquivos monitorados ▪ Reveja os resultados das atividades de monitoramento	☐	☐	☐	☐	☐
11.5.1	Há um processo implementado para responder a qualquer alerta gerado pela solução de detecção de alterações?	▪ Examine as definições de configuração do sistema	☐	☐	☐	☐	☐
11.6	As políticas de segurança e procedimentos operacionais para o teste e monitoramento da segurança são/estão: • Documentados • Em uso • Conhecidos por todas as partes envolvidas	▪ Examine as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐	☐

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/A	Não testado
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada para todas as equipes relevantes?	▪ Reveja a política de segurança de informações	☐	☐	☐	☐	☐
12.1.1	A política de segurança é revisada ao menos uma vez por ano e atualizada quando o ambiente é alterado?	▪ Reveja a política de segurança de informações ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.2	(a) Existe um processo de avaliação de risco anual implementado que • Identifique os recursos, ameaças e vulnerabilidades críticos, e • Resulte em uma análise formal, documentada de risco? *Os exemplos de metodologias de avaliação de risco incluem, entre outros, OCTAVE, ISO 27005 e NIST SP 800-30.*	▪ Reveja os processos anuais de avaliação de risco ▪ Entreviste a equipe	☐	☐	☐	☐	☐
	(b) Existe um processo de avaliação de risco realizado pelo menos anualmente e mediante alterações significativas ao ambiente (por exemplo, aquisição, fusão, relocalização etc.)?	▪ Reveja a documentação de avaliação de risco ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
12.3	O uso de políticas de tecnologias críticas é desenvolvido para definir o uso apropriado destas tecnologias e exige o seguinte: ***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.*						
12.3.1	Aprovação explícita pelas partes autorizadas para uso das tecnologias?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.2	Autenticação para o uso da tecnologia?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.3	Uma lista de todos esses dispositivos e equipes com acesso?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.4	Há um método para determinar prontamente e precisamente o proprietário, informações de contato e propósito (por exemplo, etiqueta, codificação, e/ou inventário de dispositivos)?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.5	Usos aceitáveis das tecnologias?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.6	Locais de rede aceitáveis para as tecnologias?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.7	Lista dos produtos aprovados pela empresa?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.3.8	Desconexão automática das sessões para tecnologias de acesso remoto após um período específico de inatividade?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
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?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
12.3.10	(a) No acesso da equipe aos dados do titular do cartão por meio de tecnologias de acesso remoto, a política especifica a proibição de cópia, transferência e armazenamento dos dados do titular do cartão em discos rígidos locais e mídias eletrônicas removíveis, exceto quando explicitamente autorizado para uma necessidade comercial definida? *Onde houver uma necessidade comercial autorizada, as políticas de utilização devem exigir que os dados sejam protegidos de acordo com todos os requisitos aplicáveis do PCI DSS.*	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
	(b) Para membros da equipe com autorização adequada, a política exige a proteção dos dados do titular do cartão de acordo com os Requisitos do PCI DSS?	▪ Reveja as políticas de uso ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.4	A política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todas as equipes?	▪ Reveja os procedimentos e a política de segurança ▪ Entreviste alguns dos funcionários responsáveis	☐	☐	☐	☐	☐
12.4.1	*Esse requisito aplica-se apenas a prestadores de serviços*						
12.5	(a) A responsabilidade pela segurança das informações é atribuída formalmente para uma pessoa responsável pela segurança ou para outro membro da gerência que tenha conhecimento sobre segurança?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐
	(b) As seguintes responsabilidades de gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e equipes que:						
12.5.1	Estabelecem, documentam e distribuem políticas e procedimentos de segurança?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐
12.5.2	Monitoram e analisam os alertas e as informações de segurança e os distribui para as equipes apropriadas?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐
12.5.4	Administram as contas dos usuários, incluindo adições, exclusões e modificações?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐
12.5.5	Monitoram e controlam todos os acessos aos dados?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐	☐
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?	▪ Reveja o programa de conscientização de segurança	☐	☐	☐	☐	☐
	(b) Os procedimentos do programa de conscientização da segurança incluem os itens a seguir:						
12.6.1	(a) O programa de conscientização da segurança fornece vários métodos para comunicação da conscientização e instrução da equipe (como cartazes, cartas, memorandos, treinamento baseado na Web, reuniões e promoções)? ***Observação:*** *Os métodos podem variar dependendo da função de cada funcionário e do nível de acesso aos dados do titular do cartão.*	▪ Reveja o programa de conscientização de segurança ▪ Reveja os procedimentos do programa de conscientização de segurança ▪ Reveja os registros de participação do programa de conscientização da segurança	☐	☐	☐	☐	☐
	(b) As equipes são instruídas na contratação e depois pelo menos uma vez ao ano?	▪ Examine os procedimentos e a documentação do programa de conscientização de segurança	☐	☐	☐	☐	☐
	(c) Os funcionários concluíram o treinamento de conscientização da segurança e sabem da importância da segurança dos dados do titular do cartão?	▪ Entreviste a equipe	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
12.6.2	Os membros da equipe devem reconhecer, pelo menos uma vez por ano, que leram e compreenderam a política e os procedimentos de segurança da empresa?	▪ Examine os procedimentos e a documentação do programa de conscientização de segurança	☐	☐	☐	☐	☐
12.7	Os possíveis funcionários (consulte a definição de "funcionário" no Requisito acima) são examinados antes da contratação para minimizar o risco de ataques de fontes internas? *Exemplos de verificações da formação incluem o histórico do emprego anterior, ficha criminal, histórico de crédito e verificações das referências.* ***Observação:*** *Para aqueles funcionários a serem contratados para determinadas funções, como caixas de loja, que têm acesso somente a um número do cartão por vez ao viabilizar uma transação, esse requisito é apenas uma recomendação.*	▪ Entreviste o gerenciamento do departamento de Recursos Humanos	☐	☐	☐	☐	☐
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?	▪ Reveja as políticas e procedimentos ▪ Observe os processos ▪ Reveja a lista de prestadores de serviços	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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 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.*	▪ Observe os acordos por escrito ▪ Reveja as políticas e procedimentos	☐	☐	☐	☐	☐
12.8.3	Existe um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐	☐
12.8.4	É mantido um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐	☐
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?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐	☐
12.9	*Esse requisito aplica-se apenas aos prestadores de serviços.*						
12.10	Foi implementado um plano de resposta a incidentes para incluir o seguinte, em preparação a reagir imediatamente a uma violação no sistema?						

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
12.10.1	(a) Foi criado um plano de resposta a incidentes para ser implementado em caso de violação do sistema?	▪ Reveja o plano de resposta a incidentes ▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	(b) No mínimo, o plano aborda o seguinte:						
	• Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo, no mínimo, a notificação às bandeiras?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Procedimentos de resposta específicos a incidentes?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Procedimentos de recuperação e continuidade dos negócios?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Processos de backup dos dados?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Análise dos requisitos legais para divulgação dos comprometimentos?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Abrangência e respostas de todos os componentes críticos do sistema?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
	• Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
12.10.2	O plano é revisado e testado pelo menos anualmente, incluindo todos os elementos alistados no Requisito 12.10.1?	▪ Reveja os procedimentos do plano de resposta a incidentes ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.10.3	Equipes específicas são designadas para estarem disponíveis em tempo integral para reagir aos alertas?	▪ Observe os processos ▪ Reveja as políticas ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
12.10.4	O treinamento adequado é prestado à equipe que é responsável pela resposta às falhas do sistema?	▪ Observe os processos ▪ Reveja os procedimentos do plano de resposta a incidentes ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.10.5	São incluídos alertas dos sistemas de monitoramento de segurança no plano de resposta a incidentes?	▪ Observe os processos ▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐	☐
12.10.6	Existe algum processo em vigor para modificar e aprimorar o plano de resposta a incidentes, de acordo com as lições aprendidas, para incorporar os desenvolvimentos do setor?	▪ Observe os processos ▪ Reveja os procedimentos do plano de resposta a incidentes ▪ Entreviste a equipe responsável	☐	☐	☐	☐	☐
12.11	*Esse requisito aplica-se apenas a prestadores de serviços*						

Apêndice A: Requisitos adicionais do PCI DSS

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

Esse apêndice não é usado para avaliações de comerciante.

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	**Sim com CCW**	**Não**	**N/A**	**Não testado**
A2.1	*Para terminais POS POI (e os pontos de terminação SSL/TLS ao qual eles se conectam) usando SSL e/ou TLS precoce:* • Os dispositivos são confirmados para não serem suscetíveis a qualquer façanha conhecida para SSL/TLS prematuro *Ou:* • Há um plano formal de redução de riscos e migração em vigor de acordo com a exigência 2.2?	▪ Analisar a documentação (por exemplo, documentação do fornecedor, detalhes de configuração do sistema/rede etc.) que verifica que os dispositivos POI POS não são suscetíveis a vulnerabilidades conhecidas para SSL/TLS antigo	☐	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*				
			Sim	Sim com CCW	Não	N/A	Não testado
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: ▪ 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 antigo; ▪ Descrição de processos de controle de alterações que são implementados para garantir que o SSL/TLS antigo não seja implementado 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?	▪ Rever plano de redução de riscos e migração documentado	☐	☐	☐	☐	☐
2.3	*Esse requisito aplica-se apenas a prestadores de serviços*						

Apêndice A3: Validação Suplementar de Entidades Designadas (DESV)

Este apêndice se aplica apenas a entidades designadas por uma empresa de pagamento ou adquirente que exigem uma validação adicional dos requisitos existentes do PCI DSS. Entidades que precisam validar esse apêndice devem usar o modelo de relatório suplementar DESV e atestado suplementar de conformidade para relatórios e consultar a empresa de pagamento e/ou adquirente aplicável sobre os procedimentos de envio.

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.	

Apêndice C: Explicação de não aplicabilidade

Se a coluna "N/D" (não disponível) tiver sido selecionada no questionário, use esta planilha para explicar por que o requisito relacionado não se aplica à sua organização.

Requisito	Motivo pelo qual o requisito não se aplica
Exemplo:	
3.4	Os dados do titular do cartão nunca são armazenados eletronicamente

Apêndice D: Explicação dos requisitos não testados

Se a coluna "Não testado" estiver marcada no questionário, use essa planilha para explicar por que o requisito relacionado não foi revisado como parte da avaliação.

Requisito	Descreve qual(is) parte(s) do requisito não foi(ram) testada(s)	Descreva por que os requisitos não foram testados
Exemplos:		
Requisito 12	*O Requisito 12.2 foi o único testado. Todos os outros requisitos do Requisito 12 foram excluídos.*	*Essa avaliação abrange apenas os requisitos do Evento 1 da Abordagem priorizada.*
Requisitos 1-8, 10-12	*Somente o Requisito 9 foi revisado para essa avaliação. Todos os outros requisitos foram excluídos.*	*A empresa é uma provedora de hospedagem física (CO-LO) e apenas controles de segurança física foram considerações nessa avaliação:*

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

Este AOC é baseado em resultados observados em SAQ D (Seção 2), datada de *(data de conclusão SAQ).*

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

☐	**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.
☐	**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. **Data prevista** para conformidade: 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. *Verifique junto ao seu adquirente ou à(s) empresa(s) de pagamento antes de preencher a Parte 4.*
☐	**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. *Se selecionada, preencha o seguinte:*

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)

☐	O Questionário de autoavaliação D do PCI DSS, versão *(versão do SAQ)*, foi preenchido segundo as instruções nele contidas.
☐	Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação em todos os aspectos materiais.
☐	Eu confirmei com meu fornecedor do aplicativo de pagamento que o aplicativo não armazena dados de autenticação confidenciais após a autorização.
☐	Eu li o PCI DSS e reconheço que sempre devo manter a conformidade total com o PCI DSS, conforme aplicável para o meu ambiente.

☐	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)

☐	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.
☐	As varreduras ASV estão sendo concluídas pelo fornecedor de varredura aprovado do PCI SSC *(nome do ASV)*

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 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 funcionários 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	☐	☐	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐	☐	
3	Proteger os dados armazenados do titular do cartão	☐	☐	
4	Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas	☐	☐	
5	Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus	☐	☐	
6	Desenvolver e manter sistemas e aplicativos seguros	☐	☐	
7	Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio	☐	☐	
8	Identificar e autenticar o acesso aos componentes do sistema	☐	☐	
9	Restringir o acesso físico aos dados do titular do cartão	☐	☐	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão	☐	☐	
11	Testar regularmente os sistemas e processos de segurança	☐	☐	
12	Manter uma política que aborde a segurança da informação para todas as equipes	☐	☐	

Apêndice A2	Requisitos adicionais do PCI DSS para entidades usando SSL/TLS precoce	☐	☐