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

Questionário de autoavaliação B-IP e Atestado de conformidade

Comerciantes com terminais independentes de ponto de interação (POI) PTS e com conexão IP – sem armazenamento eletrônico de dados do titular do cartão

Para uso com PCI DSS Versão 3.2

Abril de 2016

Alterações no documento

Data	Versão do PCI DSS	Revisão de SAQ	Descrição
N/D	1.0		Não utilizado.
N/D	2.0		Não utilizado.
Fevereiro de 2014	3.0		Novo SAQ para abordar os requisitos aplicáveis aos comerciantes que processam dados do titular do cartão apenas por meio de dispositivos de ponto de interação aprovados por PTS e independentes, com uma conexão IP com o processador do pagamento. O conteúdo é alinhado com os requisitos e procedimentos de teste do PCI DSS v3.0.
Abril de 2015	3.1		Atualizado para alinhar-se com a versão 3.1 do PCI DSS. Para detalhes das alterações do 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.
Abril de 2016	3.2	1.0	Atualizado para alinhar-se com o PCI DSS v 3.2. Para detalhes das mudanças de PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.1 para 3.2.*

Índice

Antes de você começar

O SAQ B-IP foi desenvolvido para abordar os requisitos aplicáveis aos comerciantes que processam dados do titular do cartão apenas por meio de dispositivos de ponto de interação (POI) aprovados por PTS e independentes, com uma conexão IP com o processador do pagamento.

Os comerciantes SAQ B-IP podem ser do tipo real (cartão presente) ou pedidos por correio/telefone (cartão não presente) e não podem armazenar dados do titular do cartão em nenhum sistema computacional.

Os comerciantes SAQ B-IP confirmam que para esse canal de pagamento:

- Sua empresa usa apenas dispositivos de ponto de interação (POI) aprovados por PTS e independentes (não incluindo SCRs) conectados via IP com seu processador de pagamento para obter as informações do cartão de pagamento dos clientes;
- Os dispositivos POI independentes e com conexão IP são validados de acordo com o programa POI PTS, conforme listado no site da PCI SSC (não incluindo SCRs);
- Os dispositivos POI independentes e com conexão IP não são conectados com quaisquer outros sistemas em seu ambiente (isso pode ser obtido via segmentação da rede a fim de isolar os dispositivos POI de outros sistemas);
- A única transmissão de dados do titular do cartão é de dispositivos POI aprovados por PTS para o processador do pagamento;
- O dispositivo POI não depende de nenhum outro dispositivo (por exemplo, computador, telefone móvel, tablet etc.) para conexão com o processador do pagamento;
- Quaisquer dados do titular do cartão que sua empresa retém estão em papel (por exemplo, relatórios ou recibos impressos), e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados do titular do cartão em formato eletrônico.

Esse SAQ não é aplicável para canais de Comércio eletrônico.

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

Etapas de conclusão da autoavaliação do PCI DSS

1. Identifique o SAQ aplicável para seu ambiente. Consulte o documento *Diretrizes e instruções do questionário de autoavaliação* no site da PCI SSC para obter informações.
2. Confirme que seu ambiente está adequadamente definido e atende aos critérios de elegibilidade para o SAQ que você está usando (como definido na Parte 2g do Atestado de conformidade).
3. Avalie seu ambiente quanto à conformidade com os requisitos de PCI DSS aplicáveis.
4. Conclua todas as seções desse documento:
    - Seção 1 (Partes 1 e 2 do AOC) – Informações de Avaliação e Sumário Executivo
    - Seção 2 – Questionário de autoavaliação do PCI DSS (SAQ B-IP)
    - 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 sobre todos os requisitos de PCI DSS • Detalhes do teste de procedimentos • Orientação sobre os controles de compensação
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/D (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.

Orientação para não aplicabilidade de determinados requisitos específicos

Apesar de várias organizações que preenchem o SAQ B-IP precisarem validar a conformidade com todos os requisitos do PCI DSS nesse SAQ, algumas organizações com modelos de negócio bastante específicos podem descobrir que alguns requisitos não se aplicam. Por exemplo, não se espera que uma empresa que não usa tecnologia sem fio de forma alguma valide a conformidade com as seções do PCI DSS que são específicas da tecnologia sem fio (por exemplo, requisitos 1.2.3, 2.1.1 e 4.1.1).

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

Exceção legal

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

Seção 1: Informações de avaliação

Instruções para Envio

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

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

Parte 1a. Informações sobre a organização do comerciante

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

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

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

Parte 2. Resumo executivo

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

☐ Varejo	☐ Telecomunicações	☐ Armazéns e Supermercados
☐ Petróleo	☐ Comércio eletrônico	☐ Pedido por correio/telefone (MOTO)
☐ Outros (especificar):		

Quais tipos de canais de pagamento seu negócio atende?	Quais canais de pagamento são abrangidos por esse SAQ?
☐ Pedido por telefone/correio (MOTO)	☐ Pedido por telefone/correio (MOTO)
☐ Comércio eletrônico	☐ Comércio eletrônico
☐ Cartão presente (face a face)	☐ Cartão presente (face a face)

Observação: *se sua organização tiver um processo ou canal de pagamento que não seja abrangido por esse SAQ, consulte seu adquirente ou empresa de pagamento sobre a validação para outros canais.*

Parte 2b. Descrição da indústria de cartões de pagamento

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

Parte 2c. Locais

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

Tipo de instalação	Número de instalações desse tipo	Localizações de instalação (por exemplo, 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 do QIR: Nome do indivíduo QIR: Descrição dos serviços prestados pelo QIR:	☐Sim ☐ Não
A sua empresa compartilha dados de titulares de cartão com qualquer provedor de serviços de terceiros (por exemplo, integrador e revendedor qualificado (QIR), gateways, processadores de pagamento, prestadores de serviços de pagamento (PSP), empresas de hospedagem de web, agentes de reserva de companhias aéreas, agentes do programa de fidelidade etc.)?	☐Sim ☐ Não

Se sim:

Nome do prestador de serviço:	**Descrição dos serviços fornecidos:**

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

Parte 2g. Qualificação para preencher o SAQ B-IP

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

☐	O comerciante usa apenas dispositivos de ponto de interação (POI) aprovados (exclui SCRs) por PTS e independentes conectados via IP ao processador de pagamento para obter as informações do cartão de pagamento dos clientes;
☐	Os dispositivos POI independentes e com conexão IP são validados de acordo com o programa POI PTS, conforme listado no site da PCI SSC (não incluindo SCRs);
☐	Os dispositivos POI independentes e com conexão IP não são conectados com quaisquer outros sistemas do ambiente do comerciante (isso pode ser obtido via segmentação da rede a fim de isolar os dispositivos POI de outros sistemas);
☐	A única transmissão de dados do titular do cartão é de dispositivos POI aprovados por PTS para o processador do pagamento;
☐	O dispositivo POI não depende de nenhum outro dispositivo (por exemplo, computador, telefone móvel, tablet etc.) para conexão com o processador do pagamento;

☐	O comerciante não armazena os dados de titulares de cartão em formato eletrônico; **e**
☐	Se o comerciante armazenar os dados do titular do cartão, esses dados só estarão em relatórios ou cópias em papel dos recibos e não serão recebidos eletronicamente.

Seção 2: Questionário de autoavaliação B-IP

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 uma rede segura

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.1.2	(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	☐	☐	☐	☐
1.1.4	(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	☐	☐	☐	☐
1.1.6	(a) Os padrões de configuração de firewall e roteador incluem uma lista documentada dos serviços, protocolos e portas, incluindo a justificativa de negócios e aprovação para cada um?	▪ Reveja o firewall e os padrões de configuração do roteador	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(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	☐	☐	☐	☐
1.2	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	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.2.3	Existem firewalls de perímetro instalados entre quaisquer redes sem fio e o ambiente de dados do titular do cartão e esses firewalls estão configurados para recusar ou permitir (se esse tráfego for necessário para fins comerciais) apenas tráfegos autorizados a partir do ambiente sem fio no ambiente de dados do titular do cartão?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
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:					
1.3.3	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 de fonte interna)	▪ 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	☐	☐	☐	☐

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

	Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
2.1	(a) Os valores-padrão entregues pelo fornecedor são sempre alterados antes de instalar um sistema na rede? *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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(c) As senhas/frases de senha padrão dos pontos de acesso são alteradas na instalação?	▪ 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 de 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	☐	☐	☐	☐
2.3	O acesso administrativo que não utiliza console, incluindo o acesso baseado na web, é criptografado conforme a seguir: ***Observação*: *onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.***					
	(a) Todos os acessos administrativos fora do console são criptografados com criptografia robusta e um método de criptografia robusta é invocado antes da solicitação da senha do administrador?	▪ 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 remotos 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	☐	☐	☐	☐

Proteger os dados do titular do cartão

Requisito 3: Proteger os dados armazenados do titular do cartão

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
3.2	(c) Os dados de autenticação confidenciais ou dados irrecuperáveis são excluídos ou restituídos após a conclusão do processo de autorização?	▪ 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/D
3.2.2	O código ou valor de verificação do cartão (número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) não é armazenado após a autorização?	▪ 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 pessoal (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	☐	☐	☐	☐
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	☐	☐	☐	☐

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
4.1	(a) São usados protocolos de segurança e criptografia fortes para proteger dados sensíveis do titular do cartão durante a transmissão através de redes abertas e públicas? ***Observação:*** *onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.* *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) Os protocolos de segurança foram implementados para usar somente configurações seguras, sem suporte para versões ou configurações não seguras?	▪ Examine as configurações do sistema	☐	☐	☐	☐
	(d) A força da criptografia adequada 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/D
4.1.1	São usadas as melhores práticas da indústria para implementar criptografia forte para a autenticação e transmissão para as redes sem fio que transmitem dados de titulares de cartão ou que estão conectadas ao ambiente de dados do titular do cartão?	▪ Reveja os padrões documentados ▪ Reveja as redes sem fio ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
4.2	(b) Existem políticas em vigor que afirmam que os PANs desprotegidos não são enviados por meio das tecnologias de envio de mensagens de usuário final?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐

Manter um programa de gerenciamento de vulnerabilidades

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

	Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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 melhores práticas do setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.* *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	☐	☐	☐	☐
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	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(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	☐	☐	☐	☐

Implemente medidas rigorosas de controle de acesso

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
7.1	O acesso aos componentes do sistema e aos dados do titular do cartão é limitado somente àquelas pessoas cuja função requer tal acesso, conforme itens a seguir:					
7.1.2	O acesso aos IDs de usuários privilegiados é restrito ao seguinte: ▪ Restrito ao menor número de privilégios necessários para o desempenho das responsabilidades da função? ▪ Permitido apenas às funções que requerem especificamente tal acesso privilegiado?	▪ Examine a política escrita de controle de acesso ▪ Entreviste a equipe ▪ Entreviste os gerentes ▪ Reveja os IDs de usuários privilegiados	☐	☐	☐	☐
7.1.3	É atribuído o acesso com base na classificação e função de trabalho do funcionário individualmente?	▪ Examine a política escrita de controle de acesso ▪ Entreviste os gerentes ▪ Reveja os IDs dos usuários	☐	☐	☐	☐

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
8.1.5	(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	☐	☐	☐	☐
	(b) As contas de acesso remoto de terceiros são monitoradas quando em uso?	▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐
8.3	Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE é protegido usando 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 autenticação multifatores.*					
8.3.2	É incorporada autenticação multifatores para todos os acessos de rede remota (usuário e administrador e incluindo o acesso de terceiros para suporte e manutenção) provenientes de fora da rede da entidade?	▪ Examine as configurações do sistema ▪ Observar os funcionários se conectando remotamente	☐	☐	☐	☐

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

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
9.1.2	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	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
9.5	Todas as mídias estão fisicamente seguras (incluindo, entre outros, computadores, mídias eletrônicas removíveis, recibos em papel, relatórios em papel e faxes)? *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	☐	☐	☐	☐
9.6	(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	☐	☐	☐	☐
9.8	(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	☐	☐	☐	☐
	(c) A destruição é executada da seguinte forma:					

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
9.8.1	(a) Os materiais impressos são fragmentados, incinerados ou reciclados, de forma que os dados do titular do cartão não possam ser reconstruídos?	▪ Reveja os procedimentos e políticas de destruição periódica de mídias ▪ Entreviste a equipe ▪ 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	☐	☐	☐	☐
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 como segue? ***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 à substituição?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐
	(c) As políticas e procedimentos exigem que os funcionários sejam treinados para reconhecer os comportamentos suspeitos e para reportar a falsificação ou substituição de dispositivos?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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 pode 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 para 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/D
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	☐	☐	☐	☐

Monitorar e testar as redes regularmente

Requisito 11: Testar regularmente os sistemas e processos de segurança

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
11.2.2	(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	☐	☐	☐	☐

Manter uma política de segurança de informações

Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada para todas as equipes relevantes?	▪ 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	☐	☐	☐	☐
12.3	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	☐	☐	☐	☐
12.3.3	Uma lista de todos esses dispositivos e equipes com acesso?	▪ 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	☐	☐	☐	☐
12.3.9	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/D
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	☐	☐	☐	☐
12.5	(b) As seguintes responsabilidades do gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e para as equipes que:					
12.5.3	Estabelecem, documentam e distribuem procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?	▪ 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	☐	☐	☐	☐
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 serviço	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
12.8.2	É mantido um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados que eles possuem do titular do cartão, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente? ***Observação:*** *as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.*	▪ 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	☐	☐	☐	☐
12.10.1	(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	☐	☐	☐	☐

Apêndice A: Requisitos adicionais do PCI DSS

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

Esse apêndice não é usado para avaliações de comerciante.

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
A2.1	*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 precoce *Ou:* • Há um plano formal de redução de riscos e migração em vigor de acordo com a exigência 2.2?	▪ Revise a documentação (por exemplo, documentação do fornecedor, detalhes de configuração do sistema/rede etc.) que verifica que dispositivos POI POS não são suscetíveis a qualquer vulnerabilidade conhecida para SSL/TLS precoce	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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 precoce; ▪ Descrição de processos de controle de alterações que são implementados para garantir que a SSL/TLS precoce não seja implementada em novos ambientes; ▪ Visão geral do plano do projeto de migração, incluindo a data de conclusão do objetivo da migração até no máximo 30 de junho de 2018?	▪ Rever plano de redução de riscos e migração documentado	☐	☐	☐	☐

Anexo A3: Validação Suplementar de Entidades Designadas (DESV)

Este anexo 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

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

Este AOC é baseado em resultados observados no SAQ B-IP (Seção 2), datado de *(data de conclusão de SAQ).*

Baseado nos resultados documentados no SAQ B-IP 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 B-IP 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 pessoal inserido pelo titular do cartão durante uma transação com cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

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

Selecione a resposta apropriada para "Conformidade com os requisitos PCI DSS" para cada requisito. Se você responder "Não" a qualquer um dos requisitos, será solicitado que a data na qual a empresa estará em conformidade seja fornecida além do requisito e de uma descrição resumida das ações que estão sendo realizadas para atender ao requisito.

Verifique junto ao seu adquirente ou à(s) empresa(s) de pagamento antes de preencher a Parte 4.

Exigência 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	☐	☐	
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	☐	☐	
11	Testar regularmente os sistemas e processos de segurança	☐	☐	
12	Manter uma política que aborde a segurança da informação para todas as equipes	☐	☐	
Anexo A2	Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS	☐	☐	

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