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

Questionário de autoavaliação A
e Atestado de conformidade

Comerciantes com cartões não presentes, todas as funções dos dados do titular do cartão são terceirizadas

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	Versão atualizada para alinhar-se com outros SAQs de numeração.
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.* Requisitos adicionados dos requisitos 2, 8 e 12 da versão 3.2 do PCI DSS.
Janeiro de 2017	3.2	1.1	Alterações foram atualizadas no documento para esclarecer os requisitos adicionados na atualização de abril de 2016. Observação adicionada à seção Antes de você começar para esclarecer o objetivo da inclusão dos requisitos 2 e 8 do PCI DSS.

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

Alterações no documento ..... **i**

Antes de você começar ..... **iii**

Etapas de conclusão da autoavaliação do PCI DSS ..... **iv**

Entendendo o Questionário de autoavaliação ..... **iv**

Teste esperado iv

Preenchendo o questionário de autoavaliação ..... **v**

Orientação para não aplicabilidade de determinados requisitos específicos ..... **v**

Exceção legal v

Seção 1: Informações de avaliação **1**

Seção 2: Questionário de autoavaliação A **5**

Construir e manter a segurança de rede e sistemas **5**

Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança *5*

Implementar medidas rigorosas de controle de acesso **6**

Requisito 8: Identificar e autenticar o acesso aos componentes do sistema *6*

Requisito 9: Restringir o acesso físico aos dados do titular do cartão *7*

Manter uma política de segurança de informações **9**

Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes *9*

Apêndice A: Requisitos adicionais do PCI DSS **11**

Apêndice A1: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada *11*

Apêndice A2: Requisitos adicionais do DSS PCI para entidades usando SSL/antigo TLS *11*

Apêndice A3: Validação Suplementar de Entidades Designadas (DESV) *11*

Apêndice B: Planilha dos controles de compensação **12**

Apêndice C: Explicação de não aplicabilidade **13**

Seção 3: Detalhes de atestado e validação **14**

Antes de você começar

O SAQ A foi desenvolvido para abordar os requisitos aplicáveis aos comerciantes cujas funções de dados do portador do cartão são completamente terceirizadas a terceiros válidos, nas quais os comerciantes retêm apenas recibos ou relatórios impressos com os dados do portador do cartão.

Os comerciantes SAQ A podem ser comércio eletrônico ou de pedido por telefone/correio (cartão não presente), e não armazenam, processam ou transmitem dados do titular do cartão em formato eletrônico em seus sistemas ou instalações.

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

- Sua empresa aceita somente transações sem a presença do cartão (comércio eletrônico ou pedidos por correio/telefone);
- Todo processamento de dados de titulares de cartão é totalmente terceirizado para prestadores de serviços de terceiros do PCI DSS validado;
- Sua empresa não armazena, processa ou transmite nenhum dado do titular do cartão nos seus sistemas e nas suas instalações, mas confia totalmente em uma empresa terceirizada para lidar com essas funções;
- Sua empresa confirmou que o fornecedor que lida com o armazenamento, processamento e/ou transmissão dos dados do titular do cartão está em conformidade com PCI DSS; **e**
- Quaisquer dados que sua empresa retiver estão em papel (por exemplo, relatórios ou recibos impressos), e estes documentos não são recebidos eletronicamente.

Adicionalmente, para canais de comércio eletrônico:

- Todos os elementos das páginas de pagamento entregues ao navegador do consumidor se originam apenas e diretamente de um prestador de serviços terceirizado do PCI DSS validado.

Esse SAQ não é aplicável a canais presenciais.

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

Observação: *Para este SAQ, os requisitos do PCI DSS que tratam da proteção dos sistemas computacionais (por exemplo, requisitos 2 e 8) aplicam-se aos comerciantes de e-commerce que redirecionam clientes dos seus sites para um terceiro para processamento de pagamento e, especificamente, para o servidor de web do comerciante no qual o mecanismo de redirecionamento está localizado. Comerciantes com pedidos por correio/telefone (MOTO) ou e-commerce que terceirizaram completamente suas operações (em que não há mecanismo de redirecionamento do comerciante para o terceiro) e que, portanto, não têm sistemas em escopo para este SAQ, considerariam estes requisitos como sendo "não aplicáveis". Consultar a orientação nas páginas seguintes sobre como comunicar requisitos que não são aplicáveis.*

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 A)
   - 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
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.

Orientação para não aplicabilidade de determinados requisitos específicos

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) ☐ Comércio eletrônico ☐ Cartão presente (face a face)	☐ 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

Liste 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.*

Parte 2g. Qualificação para Preencher o SAQ A

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

☐	O comerciante aceita somente transações sem a presença do cartão (comércio eletrônico ou pedidos por correio/telefone);
☐	Todo processamento de dados de titulares de cartão é totalmente terceirizado para prestadores de serviços de terceiros do PCI DSS validado;
☐	O comerciante não armazena, processa ou transmite nenhum dado do titular do cartão nos seus sistemas e nas suas instalações, mas confia totalmente em uma empresa terceirizada para lidar com essas funções;
☐	O comerciante confirmou que o fornecedor que lida com o armazenamento, processamento e/ou transmissão dos dados do titular do cartão está em conformidade com PCI DSS; **e**

☐	Quaisquer dados de titulares de cartão que o comerciante mantém estão em papel (por exemplo, relatórios ou recibos impressos), e esses documentos não são recebidos eletronicamente.
☐	*Adicionalmente, para canais de comércio eletrônico:* Todos os elementos das páginas de pagamento entregues ao navegador do consumidor se originam apenas e diretamente de um prestador de serviços terceirizado do PCI DSS validado.

Seção 2: Questionário de autoavaliação A

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 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
2.1	(a) Os padrões fornecidos ao vendedor 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 desabilitadas antes de instalar 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	☐	☐	☐	☐

Implementar medidas rigorosas de controle de acesso

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
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	☐	☐	☐	☐
8.1.3	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	☐	☐	☐	☐
8.2	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	☐	☐	☐	☐
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	☐	☐	☐	☐

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

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
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	☐	☐	☐	☐

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

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
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	☐	☐	☐	☐
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	☐	☐	☐	☐

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

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 DSS PCI para entidades usando SSL/antigo TLS

Esse anexo não é usado para avaliações de comerciante SAQ A.

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

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

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

Com base nos resultados documentados na SAQ A mencionado acima, os signatários identificados nas partes 3b-3d, conforme o caso, 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 A 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.

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**	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐	☐	
8	Identificar e autenticar o acesso aos componentes do sistema	☐	☐	
9	Restringir o acesso físico aos dados do titular do cartão	☐	☐	
12	Manter uma política que aborde a segurança da informação para todas as equipes	☐	☐	

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