Indústria de Cartões de Pagamento (PCI)
Padrão de Segurança de Dados

Questionário de Auto-avaliação P2PE
e Atestado de Conformidade

Comerciantes usando terminais de pagamento de hardware em um PCI SSC – apenas solução P2PE – sem armazenamento eletrônico de dados de titulares de cartão

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
N/A	1.0		Não utilizado.
Maio de 2012	2.0		Criar o SAQ P2PE-HW para comerciantes usando somente terminais de hardware como parte de uma solução P2PE validada listada pela PCI SSC. Esse SAQ é para uso com o 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*. Removido "HW" do título do SAQ, já que pode ser usado por comerciantes usando uma solução HW/HW ou HW/híbrida P2PE.
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 alterações de PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.1 para 3.2*. Requisitos 3.3 e 4.2 do PCI DSS removidos, como tratado na implementação da solução PCI P2PE e PIM.
Janeiro de 2017	3.2	1.1	As alterações no documento foram atualizadas para esclarecer os requisitos removidos na atualização de abril de 2016.

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.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Índice

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Antes de você começar

Critérios de Elegibilidade de Comerciante para SAQ P2PE

SAQ P2PE foi desenvolvido para atender às necessidades aplicáveis aos comerciantes que processam dados de titulares de cartão somente através de terminais de pagamento de hardware incluídos em uma solução de criptografia ponto a ponto (P2PE) validada e alistada em PCI.

Comerciantes SAQ P2PE não possuem acesso aos dados claros de texto de titulares de cartão em qualquer sistema de computador e apenas entram dados de conta através de terminais de pagamento de hardware a partir de uma solução P2PE aprovada por PCI SSC. Os comerciantes SAQ P2PE podem ser do tipo real (cartão presente) ou pedidos por correio/telefone (cartão não presente). Por exemplo, um comerciante de pedidos por correio/telefone pode ser elegível para SAQ P2PE se receber os dados do portador do cartão em papel ou por telefone e vinculá-lo diretamente e somente a um dispositivo de hardware P2PE validado.

Comerciantes SAQ P2PE confirmam que, para este canal de pagamento:

- Todo o processamento do pagamento é através de uma solução validada PCI P2PE aprovada e alistada pelo PCI SSC;
- Os únicos sistemas no ambiente do comerciante que armazenam, processam ou transmitem dados da conta são os dispositivos de ponto de interação (POI) que são aprovados para uso com a solução de P2PE alistada em PCI;
- Sua empresa, portanto, não recebe ou transmite dados de titulares de cartão eletronicamente;
- Não há nenhum armazenamento de dados de titulares de cartão eletrônico no ambiente;
- Se a sua empresa armazenar os dados do portador do cartão, esses dados só estarão em relatórios ou cópias em papel dos recibos e não serão recebidos eletronicamente; **e**
- Sua empresa implementou todos os controles no *Manual de instruções P2PE (PIM)* fornecido pelo provedor de soluções P2PE.

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.

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. Confirme que você implementou todos os elementos do PIM.
4. Avalie seu ambiente quanto à conformidade com os requisitos de PCI DSS aplicáveis.
5. Conclua todas as seções desse documento:
    - Seção 1 (Partes 1 e 2 do AOC – Informações de Avaliação e Resumo Executivo)
    - Seção 2 – Questionário de Autoavaliação de PCI DSS (SAQ P2PE)
    - 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)

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

6. Envie o SAQ e o Atestado de Conformidade (AOC), juntamente com qualquer outra documentação solicitada, 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.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

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.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Seção 1: Informações de avaliação

Instruções para Envio

Esse documento deve ser preenchido como uma declaração do resultado de autoavaliação do comerciante com os *Requisitos do padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS) e procedimentos da avaliação de segurança*. 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 outras bandeiras 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	☐ Pedido por correio/telefone	☐ Outros (especifique):

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)

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

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. Solução P2PE

Forneça as seguintes informações sobre a solução de PCI P2PE validada que sua organização usa:

Nome do provedor de solução P2PE:	
Nome da solução P2PE:	
Número de referência da PCI SSC	
Dispositivos P2PE POI listados utilizados pelo comerciante (dependências do dispositivo PTS):	

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?	☐ Sim ☐ Não

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

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

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, agentes de reservas aéreas, agentes do programa de fidelidade etc.)? ***Se sim:***	☐ Sim ☐ Não

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

Observação: *o requisito 12.8 aplica-se a todas as entidades listadas em resposta a essa pergunta.*

Parte 2g. Elegibilidade para preencher SAQ P2PE

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

☐	Todo o processamento do pagamento é através da solução validada de PCI P2PE aprovada e alistada pelo PCI SSC (conforme acima).
☐	Os únicos sistemas no ambiente do comerciante que armazenam, processam ou transmitem dados de conta são os dispositivos de Ponto de interação (POI) que são aprovados para uso com a solução P2PE listada pela PCI e validada.
☐	O comerciante não recebe ou transmite eletronicamente os dados do portador do cartão.
☐	O comerciante verifica que não há armazenamento de legado dos dados do portador do cartão eletrônico no ambiente.
☐	Se o comerciante armazenar os dados do portador do cartão, esses dados só estarão em relatórios ou cópias em papel dos recibos e não serão recebidos eletronicamente, **e**
☐	O comerciante implementou todos os controles no Manual de instrução P2PE (PIM) fornecido pelo provedor de solução P2PE.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Seção 2: Questionário de Autoavaliação P2PE

Observação: *as perguntas a seguir estão numeradas de acordo com os requisitos e procedimentos reais de teste do PCI DSS, conforme definido no documento* Requisitos do PCI DSS e procedimentos da avaliação de segurança*. Como apenas um subconjunto de requisitos de PCI DSS é fornecido neste SAQ P2PE, a numeração destas perguntas pode não ser consecutiva.*

Data de conclusão da autoavaliação:

Proteger os dados do titular do cartão

Requisito 3: Proteger os dados armazenados do titular do cartão

Observação: *O Requisito 3 aplica-se apenas aos comerciantes de SAQ P2PE que possuem registros em papel (por exemplo, recibos, relatórios impressos etc.) com dados de conta, incluindo números de contas principais (primary account numbers, PANs).*

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

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/A**
	(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	☐	☐	☐	☐
Orientação: *as respostas "sim" para os requisitos em 3.1 significam que se um comerciante armazena papéis (por exemplo, recibos ou relatórios impressos) que possuem dados da conta, esse comerciante somente armazenará papéis enquanto isso for necessário para fins de negócios, legais e/ou regulatórios, e destruirá os papéis assim que eles não forem mais necessários.* *Se um comerciante nunca imprime ou armazena papéis com dados de conta, esse comerciante deverá marcar a coluna "N/D" e preencher a planilha "Explicação de não aplicabilidade" no Apêndice C.*						
3.2.2	Para o armazenamento de papéis, 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 em nenhuma circunstância?	▪ Examine as fontes de dados de papel	☐	☐	☐	☐
Orientação: *uma resposta "sim" para o requisito 3.2.2 significa que se o comerciante anota o código de segurança do cartão durante uma transação, esse comerciante deve destruir de modo seguro o papel (por exemplo, com um picador de papéis) imediatamente após a conclusão da transação, ou deixar o código ilegível (por exemplo ao pintá-lo de preto com um marcador) antes de o papel ser armazenado.* *Se o comerciante nunca solicita o número de três ou quatro dígitos na frente ou atrás do cartão de pagamento ("código de segurança do cartão"), esse comerciante deve marcar a coluna "N/D" e preencher a planilha "Explicação de não aplicabilidade" no Apêndice C.*						
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	☐	☐	☐	☐
Orientação: *uma resposta "sim" ao requisito 3.7 significa que, se o comerciante armazena papéis com dados de conta, esse comerciante tem políticas e procedimentos para os requisitos 3.1, 3.2.2 e 3.3. Isso ajuda a garantir que os funcionários estão cientes e seguem as políticas de segurança e os procedimentos operacionais documentados para gerenciar o armazenamento seguro dos dados do portador do cartão continuamente.*						

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Implementar medidas rigorosas de controle de acesso

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

Observação: *os Requisitos 9.5 e 9.8 se aplicam apenas aos comerciantes SAQ P2PE que possuem registros em papel (por exemplo, recibos, relatórios impressos etc.) com dados de conta, incluindo números de contas principais (primary account numbers, PANs).*

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	☐	☐	☐	☐
9.8	(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 das mídias é realizada conforme a seguir:					
9.8.1	(a) Os materiais em cópia rígida são triturados, incinerados ou esmagados para que dados de titulares de cartão não possam ser reconstruídos?	▪ Reveja os procedimentos e políticas de destruição periódica de mídias ▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐
	(b) Os recipientes de armazenamento utilizados para materiais que contêm informações a serem destruídas são protegidos para impedir o acesso ao conteúdo?	▪ Reveja os procedimentos e políticas de destruição periódica de mídias ▪ Examine a segurança dos contêineres de armazenamento	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/A**
Orientação: *as respostas "sim" para os requisitos em 9.5 e 9.8 significam que o comerciante armazena de modo seguro quaisquer papéis com dados da conta, por exemplo, ao armazená-los em uma gaveta trancada, gabinete ou cofre, e que o comerciante destrói tais papéis quando eles não são mais necessários para fins de negócios. Isso inclui uma política ou documento escrito para os funcionários de modo que eles saibam como armazenar com segurança os papéis com dados da conta e como destruir os papéis que não são mais necessários.* *Se o comerciante nunca armazena papéis com dados de conta, esse comerciante deve marcar a coluna "N/D" e preencher a planilha "Explicação de não aplicabilidade" no Apêndice C.*						
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

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

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

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

Orientação: *as respostas "sim" aos requisitos em 9.9 significam que o comerciante tem políticas e procedimentos para os requisitos 9.9.1 – 9.9.3, e que ele mantém uma lista atual dos dispositivos, realiza inspeções periódicas dos dispositivos e treina os funcionários para que eles saibam detectar dispositivos substituídos ou falsificados.*

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/A**
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	☐	☐	☐	☐
Orientação: *uma resposta "sim" ao requisito 9.10 significa que o comerciante tem políticas e procedimentos para os requisitos 9.5, 9.8 e 9.9, conforme aplicável para seu ambiente. Isso ajuda a garantir que os funcionários estão cientes e seguem as políticas de segurança e os procedimentos operacionais documentados.*						

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Manter uma política de segurança de informações

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

Observação: o requisito 12 especifica que os comerciantes devem ter políticas de segurança de informações para seus funcionários, mas essas políticas podem ser simples ou complexas, conforme a necessidade para o tamanho e complexidade das operações do comerciante. O documento de política deve ser fornecido a todos os funcionários, para que eles estejam cientes de suas responsabilidades em proteger os terminais de pagamento, quaisquer documentos em papel com dados dos titulares de cartão etc. Se um comerciante não possui funcionários, então espera-se que o comerciante entenda e reconheça a sua responsabilidade de segurança dentro de sua loja.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/A
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	☐	☐	☐	☐
Orientação: *as respostas "sim" para os requisitos em 12.1 significam que o comerciante tem uma política de segurança razoável para o tamanho e complexidade de suas operações, e que a política é revisada anualmente e atualizada se necessário. Por exemplo, tal política pode ser um documento simples que abranja como proteger os dispositivos de pagamento e armazenamento de acordo com o* Manual de instrução P2PE (PIM) *e para quem ligar em caso de emergência.*						
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	☐	☐	☐	☐
Orientação: *Uma resposta "sim" para o requisito 12.4 significa que a política de segurança do comerciante define as responsabilidades de segurança básicas para todos os funcionários, consistente com o tamanho e complexidade das operações. Por exemplo, as responsabilidades de segurança podem ser definidas de acordo com as responsabilidades básicas pelos níveis do funcionário, como as responsabilidades esperadas de um gerente/proprietário e aquelas esperadas pelos auxiliares.*						
12.5	As seguintes responsabilidades de gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e equipes que:					

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/A**
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	☐	☐	☐	☐
Orientação: *uma resposta "sim" para o requisito 12.5.3 significa que o comerciante tem uma pessoa designada como responsável para a resposta aos incidentes e planos de escalação exigidos em 12.9.*						
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	☐	☑	☐	☐
Orientação: *uma resposta "sim" para o requisito 12.6 significa que o comerciante tem um programa de conscientização de segurança consistente com o tamanho e a complexidade de suas operações. Por exemplo, um programa de conscientização simples pode ser um folheto publicado pelo setor de administração, ou um e-mail periódico enviado para todos os funcionários. Exemplos de mensagens do programa de conscientização incluem descrições das dicas de segurança que todos os funcionários devem seguir, por exemplo, como trancar portas e contêineres de armazenamento, como determinar se um terminal de pagamento foi falsificado e como identificar funcionários legítimos que podem fazer manutenção nos terminais de pagamento de hardware.*						
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/A**
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	☐	☐	☐	☐
Orientação: *as respostas "sim" para os requisitos em 12.8 significam que o comerciante tem uma lista e acordos com os prestadores de serviços com os quais compartilha os dados do portador do cartão. Por exemplo, tais acordos seriam aplicáveis se um comerciante usar uma empresa com retenção de documentos para armazenar documentos em papel que incluem dados de conta.*						
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
		Sim	Sim com CCW	Não	N/A
Orientação: *as respostas "sim" para os requisitos em 12.10 significam que o comerciante documentou uma resposta a incidentes e um plano de escalação para uso em emergências, consistentes com o tamanho e a complexidade de suas operações. Por exemplo, tal plano pode ser um documento simples publicado no setor de administração, listando para quem ligar em diversas situações com uma revisão anual para confirmar a precisão, e também poderia abranger os procedimentos completos para um plano de respostas a incidentes, incluindo instalações "hotsite" de backup e o teste anual detalhado. Esse plano deve estar prontamente disponível para todos os funcionários como um recurso em uma emergência.*					

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Anexo 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

Este anexo não é usado para avaliações de comerciantes SAQ P2PE

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.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Anexo 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.	

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Anexo 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:	
12.8	Os dados do portador do cartão nunca são compartilhados com prestadores de serviços.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

Este AOC é baseado em resultados observados no SAQ P2PE (Seção 2), datada de *(data de conclusão de SAQ).*

Baseado nos resultados documentados no SAQ P2PE 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 ***(marque um):***

☐	**Em conformidade:** todas as seções de PCI DSS SAQ P2PE estão completas e todas as perguntas respondidas afirmativamente, resultando em uma classificação geral de **CONFORMIDADE**, assim, *(nome da empresa do comerciante)* demonstrou total conformidade com o PCI DSS.
☐	**Não conformidade:** Nem todas as seções do PCI DSS SAQ P2PE estão completas ou nem todas as perguntas estão respondidas afirmativamente, resultando em uma classificação geral de **NÃO CONFORMIDADE**, assim, *(nome da empresa do comerciante)* não demonstrou total conformidade 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 com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*
☐	**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 P2PE de autoavaliação do PCI DSS, versão *(versão do SAQ)*, foi concluído de acordo com as instruções nele contidas.
☐	Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação.
☐	Eu li o PCI DSS e reconheço que sempre devo manter a conformidade total com o PCI DSS, conforme aplicável para o meu ambiente.

Parte 3a. Reconhecimento do status (continuação)

☐	Se meu ambiente mudar, reconheço que devo reavaliá-lo e implementar quaisquer requisitos adicionais de PCI DSS que forem aplicáveis.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

☐	Não há evidências de armazenamento de dados da tarja magnética[1], dados de CAV2, CVC2, CID ou CVV2[2], ou dados de PIN[3] em QUAISQUER sistemas analisados durante essa avaliação.

Parte 3b. Atestado do comerciante

Assinatura do responsável executivo pelo comerciante ↗	*Data:*
Nome do responsável executivo pelo comerciante:	*Forma de tratamento:*

Parte 3c. Assessor de Segurança Qualificado (QSA) Reconhecimento (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 manter todos os dados da tarja magnética após a autorização da transação. Os únicos elementos dos dados de rastreamento que podem ser retidos são o número da conta, a data de vencimento e o nome.

[2] O valor de três ou quatro dígitos impresso à direita do 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 portador do cartão durante uma transação com cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.

Parte 4. Plano de ação para status de não 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 com seu adquirente ou com a(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.

Exigência do PCI DSS*	**Descrição do requisito**	**Conformidade com os requisitos do PCI DSS** (selecione um)		**Data de reparação e ações** (se "NÃO" estiver selecionado para qualquer requisito)
		SIM	**NÃO**	
3	Proteger os dados armazenados do titular do cartão	☐	☐	
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.*

© 2006-2017 PCI Security Standards Council, LLC. Todos os direitos reservados.