Payment Card Industry (PCI)

Padrão de Segurança de Dados

Atestado de conformidade para avaliações in loco – Comerciantes

Versão 3.2.1

Junho de 2018

Seção 1: Informações de avaliação

Instruções para Envio

Esse Atestado de Conformidade deve ser preenchido como uma declaração dos resultados da avaliação 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 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	☐ E-commerce	☐ Pedido por correio/telefone (MOTO)
☐ Outros (especificar):		
Quais tipos de canais de pagamento seu negócio atende? ☐ Pedido por telefone/correio (MOTO) ☐ E-Commerce ☐ Cartão presente (face a face)	Quais canais de pagamento são abrangidos por essa avaliação? ☐ Pedido por telefone/correio (MOTO) ☐ E-Commerce ☐ Cartão presente (face a face)	

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

Parte 2b. Descrição da indústria de cartões de pagamento

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

Parte 2c. Locais

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

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

Parte 2d. Aplicativo de pagamento

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

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

Nome do aplicativo de pagamento	Número da versão	Fornecedor do aplicativo	O aplicativo está listado no PA-DSS?	Data de expiração da listagem PA-DSS (se aplicável)
			☐ Sim ☐ Não	
			☐ Sim ☐ Não	
			☐ Sim ☐ Não	
			☐ Sim ☐ Não	
			☐ Sim ☐ Não	

Parte 2e. Descrição do ambiente

Forneça uma descrição de ***alto nível*** do ambiente abrangido por essa avaliação. *Por exemplo:* • *Conexões dentro e fora do ambiente de dados do titular do cartão (CDE).*	

• *Os componentes de sistema críticos no CDE, como dispositivos POS, banco de dados, servidores da web etc, e quaisquer outros componentes de pagamentos necessários, conforme aplicável.*	
Seu negócio usa segmentação de rede para afetar o escopo do seu ambiente de PCI DSS? *(Consulte a seção "Segmentação de rede" do PCI DSS para obter orientação sobre a segmentação de rede)*	☐ Sim ☐ Não

Parte 2f. Prestadores de serviços de terceiros

Sua empresa usa um integrador e revendedor qualificado (QIR)? Se sim: Nome da empresa QIR: Nome do Indivíduo QIR: Descrição dos serviços prestados pelo QIR:	☐ Sim ☐ Não
A sua empresa compartilha dados de titulares de cartão com qualquer provedor de serviços de terceiros (por exemplo, integrador e revendedor qualificado (QIR), gateways, processadores de pagamento, prestadores de serviços de pagamento (PSP), empresas de hospedagem de web, agentes de reserva de companhias aéreas, agentes do programa de fidelidade, etc.)?	☐ Sim ☐ Não

Se sim:

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

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

Seção 2: Relatório de conformidade

Esse Atestado de Conformidade reflete os resultados de uma avaliação in loco, sendo documentado em um ROC (Relatório de Conformidade) de acompanhamento.

A avaliação documentada neste atestado e no ROC foi concluída em:	
Controles de compensação foram usados para atender qualquer requisito no ROC?	☐ Sim ☐ Não
Algum requisito no ROC foi identificado como não aplicável (N/A)?	☐ Sim ☐ Não
Algum requisito não foi testado?	☐ Sim ☐ Não
Algum requisito no ROC não foi possível de ser atendido devido a uma restrição legal?	☐ Sim ☐ Não

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

Este AOC é baseado em resultados observados no ROC, datado de (*data de conclusão do ROC).*

Baseado nos resultados documentados no ROC 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 do PCI DSS ROC 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 PCI DSS ROC 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 alocados" 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 ROC foi concluído de acordo com as exigências e os *procedimentos de avaliação de segurança do PCI DSS versão (número da versão)* e foi concluído de acordo com as instruções pertinentes.
☐	Todas as informações contidas no ROC mencionado anteriormente e neste atestado representam adequadamente os resultados da 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. 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 reter esses dados de tarja magnética após a autorização da transação. Os únicos elementos dos dados da tarja magnética que podem ser retidos são o número da conta principal (PAN), o nome do titular do cartão e a data de vencimento.

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

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

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

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

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

Requisito do PCI DSS	**Descrição do requisito**	**Em conformidade com os requisitos do PCI DSS** *(selecione um)*		**Data de reparação e ações** (se "NÃO" estiver selecionado para qualquer requisito)
		SIM	**NÃO**	
1	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão	☐	☐	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐	☐	
3	Proteger os dados armazenados do portador do cartão	☐	☐	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas	☐	☐	
5	Proteja todos os sistemas contra malware e atualizar regularmente programas ou software antivírus	☐	☐	
6	Desenvolver e manter sistemas e aplicativos seguros	☐	☐	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios	☐	☐	
8	Identifique e autentique o acesso aos componentes do sistema	☐	☐	
9	Restringir o acesso físico aos dados do portador do cartão	☐	☐	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão	☐	☐	
11	Testar regularmente os sistemas e processos de segurança	☐	☐	
12	Mantenha uma política que aborde a segurança da informação para todas as equipes	☐	☐	

Apêndice A2	Requisitos adicionais do PCI DSS para entidades que usam SSL/TLS antigo para conexões de terminais de POS POI com cartão presente	☐	☐