

Indústria de Cartões de Pagamento (PCI) Padrão de segurança de dados

Atestado de conformidade para Avaliações in loco – Prestadores de serviços

Versão 3.2

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.

Seção 1: Informações de avaliação

Instruções para Envio

Esse Atestado de Conformidade deve ser preenchido como uma declaração dos resultados da avaliação do prestador de serviço 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 prestador de serviço é responsável por garantir que todas as seções sejam preenchidas pelas partes relevantes, se aplicável. Entre em contato com a empresa de pagamento solicitante para obter informações sobre procedimentos de envio e relatório.

Parte 1. Informações do prestador de serviços e do assessor de segurança qualificado

Parte 1a. Informações sobre a organização do prestador de serviços

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. Verificação do escopo

Serviços que foram INCLUÍDOS no escopo da avaliação do PCI DSS (marque todas as opções que se aplicam):

Nome do(s) serviço(s) avaliado(s):

Tipo do(s) serviço(s) avaliado(s):

Provedor de hospedagem:

- Aplicativos/software
- Hardware
- Infraestrutura/rede
- Espaço físico (co-locação)
- Armazenamento
- Web
- Serviços de segurança
- Provedor de hospedagem segura 3-D
- Provedor de hospedagem compartilhada
- Outra hospedagem (especifique):

Serviços gerenciados (especifique):

- Serviços de segurança dos sistemas
- Suporte de TI
- Segurança física
- Sistema de gerenciamento de terminal
- Outros serviços (especifique):

Processamento do pagamento:

- POS/cartão presente
- internet/comércio eletrônico
- MOTO/Central de atendimento
- Caixa eletrônico
- Outro processamento (especifique):

Gerenciamento de contas

Fraude e cobrança

Gateway/switch de pagamento

Serviços de back-office

Processamento de emissões

Serviços com pagamento adiantado

Gerenciamento do faturamento

Programas de fidelidade

Gerenciamento de registros

Compensação e liquidação

Serviços do comerciante

Taxas/pagamentos para o governo

Provedor de rede

Outros (especifique):

Observação: Essas categorias são fornecidas apenas para assistência, e não são para limitar ou predeterminar a descrição do serviço de uma entidade. Se você sente que essas categorias não se aplicam a seu serviço, preencha "Outros". Se não tiver certeza se uma categoria pode ser aplicada a seu serviço, consultar com a empresa de pagamento aplicável.

Parte 2a. Verificação de Escopo (continuação)

Serviços que são fornecidos pelo prestador de serviços, mas NÃO ESTÃO INCLUÍDOS no escopo da avaliação do PCI DSS (selecione todos os que se aplicam):

Nome do(s) serviço(s) não avaliado(s):

Tipo do(s) serviço(s) não avaliado(s):

Provedor de hospedagem:

- Aplicativos/software
- Hardware
- Infraestrutura/rede
- Espaço físico (co-locação)
- Armazenamento
- Web
- Serviços de segurança
- Provedor de hospedagem segura 3-D
- Provedor de hospedagem compartilhada
- Outra hospedagem (especifique):

Serviços gerenciados (especifique):

- Serviços de segurança dos sistemas
- Suporte de TI
- Segurança física
- Sistema de gerenciamento de terminal
- Outros serviços (especifique):

Processamento do pagamento:

- POS/cartão presente
- internet/comércio eletrônico
- MOTO/Central de atendimento
- Caixa eletrônico
- Outro processamento (especifique):

Gerenciamento de contas

Fraude e cobrança

Gateway/switch de pagamento

Serviços de back-office

Processamento de emissões

Serviços com pagamento adiantado

Gerenciamento do faturamento

Programas de fidelidade

Gerenciamento de registros

Compensação e liquidação

Serviços do comerciante

Taxas/pagamentos para o governo

Provedor de rede

Outros (especifique):

Forneça uma explicação breve do motivo pelo qual os serviços selecionados não foram incluídos na avaliação:

Parte 2b. Descrição da indústria de cartões de pagamento

Descreva como e em qual capacidade seu negócio armazena, processa e/ou transmite dados do titular do cartão.

Descreva como e em qual capacidade seu negócio está envolvido ou tem a capacidade de impactar a segurança dos dados do titular do cartão.

Parte 2c. Locais

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

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

Parte 2d. Aplicativos 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)
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> Não	
			<input type="checkbox"/> Sim <input type="checkbox"/> 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 possui relação com um revendedor integrador e qualificado (QIR) com a finalidade de validar os serviços?

Sim Não

Se sim:

Nome da empresa QIR:

Nome do Indivíduo QIR :

Descrição dos serviços prestados pelo QIR:

Sua empresa possui relação com um ou mais prestadores de serviços de terceiros (por exemplo, revendedor integrador qualificado (QIR), gateways, processadores de pagamento, prestadores de serviços de pagamento (PSP), empresas de hospedagem na web, agentes de reserva de passagem aérea, agentes do programa de fidelidade etc.) com o objetivo de que os serviços sejam validados?

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. Resumo dos requisitos testados

Para cada requisito do PCI DSS, selecione um dos seguintes itens:

- **Completo** – O requisito e todos os sub-requisitos foram avaliados para tal requisito, e nenhum sub-requisito foi marcado como "Não testado" ou "Não aplicado" no ROC.
- **Parcial** – Um ou mais sub-requisitos de tal requisito foram marcados como "Não testado" ou "Não aplicável" no ROC.
- **Nenhum** – Todos os sub-requisitos de tal requisito foram marcados como "Não testado" e/ou "Não aplicável" no ROC.

Para todos os requisitos identificados como "Parcial" ou "Nenhum", forneça detalhes na coluna "Justificativa para abordagem", incluindo:

- Detalhes dos sub-requisitos específicos que foram marcados como "Não testado" e/ou "Não aplicável" no ROC
- O motivo pelo qual o(s) requisito(s) não foi(ram) testado(s) ou não é(são) aplicável(is)

Observação: Uma tabela para ser preenchida para cada serviço abrangido por esse AOC. Cópias adicionais dessa seção estão disponíveis no site da PCI SSC.

Nome do serviço avaliado:		Detalhes dos requisitos avaliados		
Requisito do PCI DSS	Completo	Parcial	Nenhum	Justificativa para abordagem (Necessária para todas as respostas "Parcial" e "Nenhum". Identifique quais sub-requisitos não foram testados e o motivo).
Requisito 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 12:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Apêndice A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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?	<input type="checkbox"/> <i>Sim</i> <input type="checkbox"/> Não
Algum requisito no ROC foi identificado como não aplicável (N/A)?	<input type="checkbox"/> <i>Sim</i> <input type="checkbox"/> Não
Algum requisito não foi testado?	<input type="checkbox"/> <i>Sim</i> <input type="checkbox"/> Não
Algum requisito no ROC não foi possível de ser atendido devido a uma restrição legal?	<input type="checkbox"/> <i>Sim</i> <input type="checkbox"/> 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 prestador de serviços)* 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 prestador de serviços)* 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 à(s) bandeira(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 magnética¹, dados de CAV2, CVC2, CID ou CVV2², ou dados de PIN³ 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 prestador de serviço

Assinatura do responsável executivo pelo prestador de serviços ↑

Date:

Nome do responsável executivo pelo prestador de serviços:

Cargo:

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 funcionário 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 à(s) bandeira(s) de pagamento aplicáveis antes de preencher a Parte 4.

Requisito do PCI DSS	Descrição do requisito	Em conformidade com os requisitos do PCI DSS (selecione um)		Data de reparação e ações (se "NÃO" estiver selecionado para qualquer requisito)
		SIM	NÃO	
1	Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteger os dados armazenados do titular do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
4	Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desenvolver e manter sistemas e aplicativos seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identificar e autenticar o acesso aos componentes do sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir o acesso físico aos dados do titular do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
11	Testar regularmente os sistemas e processos de segurança	<input type="checkbox"/>	<input type="checkbox"/>	
12	Manter uma política que aborde a segurança da informação para todas as equipes	<input type="checkbox"/>	<input type="checkbox"/>	
Apêndice A1	Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada	<input type="checkbox"/>	<input type="checkbox"/>	
Apêndice A2	Requisitos adicionais do PCI DSS para entidades usando SSL/TLS precoce	<input type="checkbox"/>	<input type="checkbox"/>	

