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

Questionário de autoavaliação A-EP e Atestado de conformidade

Comerciantes de comércio eletrônico parcialmente terceirizados usando um site de terceiros para processamento de pagamento

Para uso com o PCI DSS versão 3.2

Abril de 2016

Alterações no documento

Data	Versão do PCI DSS	Revisão de SAQ	Descrição
N/D	1.0		Não utilizado.
N/D	2.0		Não utilizado.
Fevereiro de 2014	3.0		Novo SAQ para atender às necessidades aplicáveis aos comerciantes de comércio eletrônico com um site que em si não recebe dados de titulares de cartão, mas que afeta a segurança da operação de pagamento e/ou a integridade da página que aceita dados de titulares de cartão do consumidor. O conteúdo é alinhado com os requisitos e procedimentos de teste do PCI DSS v3.0.
Abril de 2015	3.1		Atualizado para alinhar-se com a versão 3.1 do PCI DSS. Para detalhes das alterações do PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.0 para 3.1*.
Junho de 2015	3.1		Atualize o Requisito 11.3 para corrigir o erro.
Julho de 2015	3.1	1.1	Atualizado para remover as referências às "melhores práticas" antes de 30 de junho de 2015 e remover a opção de relatório de versão 2 do PCI DSS para Requisito 11.3
Abril de 2016	3.2	1.0	Atualizado para alinhar-se com o PCI DSS v 3.2. Para detalhes das mudanças de PCI DSS, consulte *PCI DSS – Resumo das Alterações de PCI DSS versão 3.1 para 3.2.*

Índice

Antes de você começar

O SAQ A-EP foi desenvolvido para abordar os requisitos aplicáveis aos comerciantes de comércio eletrônico com sites que não recebem dados do titular do cartão, mas que afetam a segurança da transação de pagamento e/ou integridade da página que aceita os dados do titular do cartão.

Os comerciantes SAQ A-EP são comerciantes de comércio eletrônico que terceirizam parcialmente o canal de pagamento de comércio eletrônico para terceiros validados por PCI DSS e não armazenam, processam ou transmitem eletronicamente os dados do titular do cartão em seus sistemas ou instalações.

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

- Sua empresa aceita apenas transações de comércio eletrônico;
- Todo o processamento de dados dos titulares de cartão, com exceção da página de pagamento, é totalmente terceirizado para um processador validado de pagamento de terceiros do PCI DSS;
- Seu site de comércio eletrônico não recebe dados do titular do cartão, mas controla como os clientes ou dados do titular do cartão são redirecionados a um processador de pagamento validado por PCI DSS;
- Se o site do comerciante for hospedado por um fornecedor terceirizado, o fornecedor é validado por todos os requisitos aplicáveis do PCI DSS (por exemplo, incluindo o Apêndice A do PCI DSS, se o fornecedor for um fornecedor de hospedagem compartilhada);
- Cada elemento da página de pagamento entregue ao navegador do consumidor origina-se do site do comerciante ou de um prestador de serviços compatível com o PCI DSS;
- 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.

Esse SAQ é aplicável apenas a canais de comércio eletrônico.

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

Observação: *para efeitos deste SAQ, os requisitos do PCI DSS que se referem ao "ambiente de dados do titular do cartão" são aplicáveis ao site do comerciante. Isso ocorre porque o site do comerciante impacta diretamente o modo como os dados do cartão de pagamento são transmitidos, mesmo que o próprio site não receba dados do titular do cartão.*

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-EP)
    - 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/D (Não disponível)	O requisito não é aplicável ao ambiente da organização (consulte a *Orientação para não aplicabilidade de determinados requisitos específicos* abaixo para ver exemplos). Todas as respostas nessa coluna exigem uma explicação de suporte no Apêndice C do SAQ.

Orientação para não aplicabilidade de determinados requisitos específicos

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

Exceção legal

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

Seção 1: Informações de avaliação

Instruções para Envio

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

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

Parte 1a. Informações sobre a organização do comerciante

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

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

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

Parte 2. Resumo executivo

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

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

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

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

Parte 2b. Descrição da indústria de cartões de pagamento

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

Parte 2c. Locais

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

Se sim:

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

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

Parte 2g. Qualificação para preencher o SAQ A-EP

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

☐	O comerciante aceita apenas transações de comércio eletrônico;
☐	Todo o processamento de dados dos titulares de cartão, com exceção da página de pagamento, é totalmente terceirizado para um processador validado de pagamento de terceiros do PCI DSS;
☐	O site de comércio eletrônico do comerciante não recebe dados do portador do cartão, mas controla como os clientes ou os dados do portador do cartão são redirecionados a um processador de pagamento validado por PCI DSS;
☐	Se o site do comerciante for hospedado por um fornecedor terceirizado, o fornecedor é validado por todos os requisitos aplicáveis do PCI DSS (por exemplo, incluindo o Apêndice A do PCI DSS, se o fornecedor for um fornecedor de hospedagem compartilhada);
☐	Cada elemento da página de pagamento entregue ao navegador do consumidor origina-se do site do comerciante ou de um prestador de serviços compatível com o PCI DSS;
☐	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.

Seção 2: Questionário de autoavaliação A-EP

Observação: *as perguntas a seguir estão numeradas de acordo com os requisitos e procedimentos de teste do PCI DSS, conforme definido no documento* Requisitos do PCI DSS e procedimentos da avaliação de segurança*.*

Data de conclusão da autoavaliação:

Construir e manter uma rede segura

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.1	Os padrões de configuração do firewall e do roteador foram estabelecidos e implementados para incluir o seguinte:					
1.1.1	Existe um processo formal para aprovar e testar todas as conexões de rede e alterações nas configurações do firewall e do roteador?	▪ Reveja o processo documentado ▪ Entreviste a equipe ▪ Examine as configurações da rede	☐	☐	☐	☐
1.1.2	(a) Há um diagrama de rede atual que identifica todas as conexões entre o ambiente dos dados do titular do cartão e outras redes, incluindo qualquer rede sem fio?	▪ Reveja o diagrama de rede atual ▪ Examine as configurações da rede	☐	☐	☐	☐
	(b) Existe um processo para assegurar que o diagrama é mantido atualizado?	▪ Entreviste a equipe responsável	☐	☐	☐	☐
1.1.3	(a) Existe um diagrama atual que mostra todos os fluxos de dados de titulares de cartão entre os sistemas e redes?	▪ Reveja o diagrama atual de fluxo de dados ▪ Examine as configurações da rede	☐	☐	☐	☐
	(b) Existe um processo para assegurar que o diagrama é mantido atualizado?	▪ Entreviste a equipe	☐	☐	☐	☐
1.1.4	(a) Um firewall é exigido e implementado em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna?	▪ Reveja os padrões de configuração do firewall ▪ Observe as configurações de rede para verificar se o firewall está instalado	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(b) O diagrama de rede atual está de acordo com os padrões de configuração do firewall?	▪ Compare os padrões de configuração do firewall com o diagrama de rede atual	☐	☐	☐	☐
1.1.6	(a) Os padrões de configuração de firewall e roteador incluem uma lista documentada dos serviços, protocolos e portas, incluindo a justificativa de negócios e aprovação para cada um?	▪ Reveja o firewall e os padrões de configuração do roteador	☐	☐	☐	☐
	(b) Todos os serviços, protocolos e portas não seguros estão identificados e existem recursos de segurança documentados e implementados para cada um desses serviços identificados?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.1.7	(a) Os padrões de configuração de firewall e roteador exigem revisão do conjunto de regras do firewall e roteador pelo menos a cada seis meses?	▪ Reveja o firewall e os padrões de configuração do roteador	☐	☐	☐	☐
	(b) Os conjuntos de regras de firewall e roteador são revistos pelo menos a cada seis meses?	▪ Examine a documentação das análises do firewall	☐	☐	☐	☐
1.2	As configurações do firewall e do roteador restringem as conexões entre redes não confiáveis e qualquer sistema no ambiente de dados do titular do cartão, da seguinte forma: ***Observação:*** *uma "rede não confiável" é qualquer rede que seja externa às redes que pertencem à entidade em análise e/ou que esteja além da capacidade da entidade de controlar ou gerenciar.*					
1.2.1	(a) O tráfego de entrada e saída é restrito ao necessário para o ambiente de dados do titular do cartão?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
	(b) Todos os outros tráfegos de entrada e saída são recusados de forma específica (como ao usar a opção explícita "recusar todos" ou uma recusa implícita após a declaração de permissão)?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.2.2	Os arquivos de configuração do roteador estão seguros em relação ao acesso não autorizado e sincronizado—por exemplo, a configuração em execução (ou ativa) corresponde à configuração inicial (usada quando as máquinas são iniciadas)?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine os arquivos de configuração do roteador e as configurações do roteador	☐	☐	☐	☐
1.2.3	Existem firewalls de perímetro instalados entre quaisquer redes sem fio e o ambiente de dados do titular do cartão e esses firewalls estão configurados para recusar ou permitir (se esse tráfego for necessário para fins comerciais) apenas tráfegos autorizados a partir do ambiente sem fio no ambiente de dados do titular do cartão?	▪ Reveja o firewall e os padrões de configuração do roteador ▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.3	O acesso público direto é proibido entre a internet e qualquer componente do sistema no ambiente de dados do titular do cartão, da seguinte forma:					
1.3.1	Existe uma DMZ implementada para limitar o tráfego de entrada somente para componentes do sistema que fornecem serviços, portas e protocolos autorizados acessíveis publicamente?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.3.2	O tráfego de internet de entrada está limitado ao endereço IP dentro da DMZ?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.3.3	As medidas contra falsificação estão implementadas para detectar e impedir que endereços IP de fonte falsificada entrem na rede? (Por exemplo, bloquear tráfego originado da internet com um endereço de fonte interna)	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.3.4	O tráfego de saída do ambiente de dados do titular do cartão para a internet está explicitamente autorizado?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
1.3.5	São permitidas apenas as conexões estabelecidas na rede?	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.3.7	(a) Existem métodos em vigor para evitar a divulgação de endereços IP privados e de informações de roteamento para a internet? ***Observação:*** *os métodos para ocultar o endereço IP podem incluir, entre outros:* • *Conversão de endereços de rede (NAT)* • *Implementação dos servidores contendo dados do titular do cartão atrás dos servidores de proxy/firewalls* • *Remoção ou filtragem das propagandas de rota para redes privadas que empregam endereçamento registrado* *Uso interno do espaço de endereço RFC1918 em vez de endereço registrado*.	▪ Examine o firewall e as configurações do roteador	☐	☐	☐	☐
	(b) A divulgação dos endereços IP privados e das informações de roteamento para entidades externas é autorizada?	▪ Examine o firewall e as configurações do roteador ▪ Entreviste a equipe	☐	☐	☐	☐
1.4	(a) Está instalado e ativo um software de firewall pessoal (ou funcionalidade equivalente) em qualquer dispositivo portátil (incluindo da empresa e/ou de propriedade dos funcionários) que se conectam à internet quando fora da rede (por exemplo, laptops usados pelos funcionários), e que também são usados para acessar o CDE?	▪ Reveja as políticas e padrões de configuração ▪ Examine os dispositivos móveis e/ou de propriedade do funcionário	☐	☐	☐	☐
	(b) O software de firewall pessoal (ou funcionalidade equivalente) é configurado para definições de configuração específicas, funcionando ativamente e não alterável por usuários de dispositivos móveis e/ou de propriedade dos funcionários?	▪ Reveja as políticas e padrões de configuração ▪ Examine os dispositivos móveis e/ou de propriedade do funcionário	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
1.5	Os procedimentos operacionais e as políticas de segurança para gerenciar os firewalls são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas?	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
2.1	(a) Os valores-padrão entregues pelo fornecedor são sempre alterados antes de instalar um sistema na rede? *Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando, às utilizadas pelos sistemas operacionais, softwares que fornecem serviços de segurança, aplicativos e contas do sistema, terminais de ponto de venda (POS), solicitações de pagamento, sequências de comunidade de Protocolo de Gerenciamento de Rede Simples (SNMP), etc.*	▪ Reveja as políticas e procedimentos ▪ Examine a documentação do fornecedor ▪ Observe as configurações do sistema e as definições da conta ▪ Entreviste a equipe	☐	☐	☐	☐
	(b) As contas padrão desnecessárias são removidas ou desativadas antes da instalação de um sistema na rede?	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema e as definições da conta ▪ Entreviste a equipe	☐	☐	☐	☐
2.2	(a) Os padrões de configuração são desenvolvidos para todos os componentes do sistema e estão de acordo com os padrões de fortalecimento do sistema aceitos pelo setor? *As fontes para os padrões de fortalecimento do sistema aceitas pelo setor incluem, entre outras, o SysAdmin Audit Network Security (SANS) Institute, o National Institute of Standards Technology (NIST), o International Organization for Standardization (ISO) e o Center for internet Security (CIS).*	▪ Reveja os padrões de configuração do sistema ▪ Reveja os padrões de fortalecimento aceitos pelo setor ▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐
	(b) Os padrões de configuração do sistema são atualizados quando novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.1?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/D**
	(c) Os padrões de configuração do sistema são aplicados quando novos sistemas são configurados?	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe	☐	☐	☐	☐
	(d) Os padrões de configuração do sistema incluem todos os seguintes itens: • Alteração de todos os padrões informados pelo fornecedor e eliminação de contas padrão desnecessárias? • Implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? • Habilitar apenas serviços, protocolos, daemons, etc. necessários, conforme exigido para a função do sistema? • Recursos de segurança adicionais são implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros? • Os parâmetros de segurança do sistema são configurados para impedir o uso incorreto? • Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários são removidas?	▪ Reveja os padrões de configuração do sistema	☐	☐	☐	☐
2.2.1	(a) Há a implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? *Por exemplo, servidores da Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.*	▪ Examine as configurações do sistema	☐	☐	☐	☐
	(b) Se forem usadas tecnologias de virtualização, somente uma função principal está implementada por componente ou dispositivo do sistema virtual?	▪ Examine as configurações do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
2.2.2	(a) Somente os serviços, protocolos e daemons necessários, entre outros, são ativados conforme a necessidade para a função do sistema (ou seja, os serviços e protocolos que não são diretamente necessários para a execução da função especificada do dispositivo estão desativados)?	▪ Reveja os padrões de configuração ▪ Examine as configurações do sistema	☐	☐	☐	☐
	(b) Todos os protocolos, daemons ou serviços não seguros e ativados são justificados de acordo com os padrões de configuração documentados?	▪ Reveja os padrões de configuração ▪ Entreviste a equipe ▪ Examine as definições de configuração ▪ Compare serviços ativos, etc, com justificativas documentadas	☐	☐	☐	☐
2.2.3	Recursos de segurança adicionais são documentados e implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros? ***Observação:*** *onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.*	▪ Reveja os padrões de configuração ▪ Examine as definições de configuração ▪ Examine as definições de configuração	☐	☐	☐	☐
2.2.4	(a) Os administradores do sistema e/ou equipes que configuram os componentes do sistema estão bem-informados sobre as configurações comuns dos parâmetros de segurança para esses componentes do sistema?	▪ Entreviste a equipe	☐	☐	☐	☐
	(b) As configurações comuns dos parâmetros de segurança estão incluídas nos padrões de configuração do sistema?	▪ Reveja os padrões de configuração do sistema	☐	☐	☐	☐
	(c) As configurações dos parâmetros de segurança estão definidas corretamente nos componentes do sistema?	▪ Examine os componentes do sistema ▪ Examine as definições de parâmetro de segurança ▪ Compare as definições com os padrões de configuração do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
2.2.5	(a) Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários foram removidas?	▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐
	(b) As funções ativadas estão documentadas e oferecem suporte para uma configuração segura?	▪ Reveja a documentação ▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐
	(c) Existem somente funcionalidades registradas presentes nos componentes do sistema?	▪ Reveja a documentação ▪ Examine os parâmetros de segurança nos componentes do sistema	☐	☐	☐	☐
2.3	Os acessos administrativos fora do console estão criptografados da seguinte forma: ***Observação*:** *onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.*					
	(a) Todos os acessos administrativos fora do console são criptografados com criptografia robusta e um método de criptografia robusta é invocado antes da solicitação da senha do administrador?	▪ Examine os componentes do sistema ▪ Examine as configurações do sistema ▪ Observe o logon de um administrador	☐	☐	☐	☐
	(b) Os serviços do sistema e os arquivos de parâmetros são configurados para prevenir o uso de Telnet e outros comandos de logon remoto não seguros?	▪ Examine os componentes do sistema ▪ Examine os serviços e arquivos	☐	☐	☐	☐
	(c) O acesso do administrador às interfaces de gerenciamento baseadas na Web é criptografado com uma criptografia robusta?	▪ Examine os componentes do sistema ▪ Observe o logon de um administrador	☐	☐	☐	☐

Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
		Sim	**Sim com CCW**	**Não**	**N/D**
(d) Para a tecnologia em uso, a criptografia robusta é implementada de acordo com as melhores práticas do setor e/ou recomendações do fornecedor?	▪ Examine os componentes do sistema ▪ Reveja a documentação do fornecedor ▪ Entreviste a equipe	☐	☐	☐	☐

Proteger os dados do portador do cartão

Requisito 3: Proteger os dados armazenados do portador do cartão

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
3.2	(c) Os dados de autenticação confidenciais ou dados irrecuperáveis são excluídos ou restituídos após a conclusão do processo de autorização?	▪ Reveja as políticas e procedimentos ▪ Examine as configurações do sistema ▪ Examine os processos de exclusão	☐	☐	☐	☐
	(d) Todos os sistemas cumprem os seguintes requisitos em relação ao não armazenamento de dados de autenticação confidenciais após a autorização (mesmo se criptografados):					
3.2.2	O código ou valor de verificação do cartão (número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) não é armazenado após a autorização?	▪ Examine as fontes de dados, incluindo: • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados	☐	☐	☐	☐
3.2.3	Após a autorização, o número de identificação pessoal (PIN) ou o bloqueio de PIN criptografado não é armazenado?	▪ Examine as fontes de dados, incluindo: • Dados de transação de entrada • Todos os registros • Arquivos do histórico • Arquivos de rastreamento • Esquema de banco de dados • Conteúdo de banco de dados	☐	☐	☐	☐

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
4.1	(a) São usados protocolos de segurança e criptografia fortes para proteger dados sensíveis do titular do cartão durante a transmissão através de redes abertas e públicas? ***Observação:*** *onde SSL/antigo TLS for utilizado, os requisitos do apêndice A2 devem ser atendidos.* *Exemplos de redes abertas e públicas incluem, entre outros, internet, tecnologias sem fio, incluindo 802.11 e bluetooth, tecnologias de celular, por exemplo, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) e General Packet Radio Service (GPRS).*	▪ Reveja os padrões documentados ▪ Reveja as políticas e procedimentos ▪ Reveja todos os locais em que o CHD é transmitido ou recebido ▪ Examine as configurações do sistema	☐	☐	☐	☐
	(b) São aceitas apenas chaves e/ou certificados confiáveis?	▪ Observe as transmissões de entrada e saída ▪ Examine as chaves e certificados	☐	☐	☐	☐
	(c) Os protocolos de segurança foram implementados para usar somente configurações seguras, sem suporte para versões ou configurações não seguras?	▪ Examine as configurações do sistema	☐	☐	☐	☐
	(d) A força da criptografia adequada foi implementada para a metodologia de criptografia em uso (verifique as recomendações/melhores práticas do fornecedor)?	▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(e) Para implementações de TLS, o TLS é habilitado sempre que dados de titulares de cartão são transmitidos ou recebidos? *Por exemplo, para implementações com base no navegador:* • *O "HTTPS" aparece como parte do protocolo de Universal Record Locator (URL) do navegador, e* • *Os dados do titular do cartão são exigidos somente se o "HTTPS" aparece como parte do URL.*	▪ Examine as configurações do sistema	☐	☐	☐	☐
4.2	(b) Existem políticas em vigor que afirmam que os PANs desprotegidos não são enviados por meio das tecnologias de envio de mensagens de usuário final?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐
4.3	As políticas de segurança e procedimentos operacionais para transmissão criptografada de dados do titular do cartão são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas?	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐

Manter um programa de gerenciamento de vulnerabilidades

Requisito 5: Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
5.1	Os softwares antivírus estão implementados em todos os sistemas normalmente afetados por softwares mal-intencionados?	▪ Examine as configurações do sistema	☐	☐	☐	☐
5.1.1	Todos os programas antivírus podem detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados (como vírus, trojans, worms, spywares, adwares e rootkits)?	▪ Reveja a documentação do fornecedor ▪ Examine as configurações do sistema	☐	☐	☐	☐
5.1.2	São executadas avaliações periódicas para identificar e avaliar a evolução de ameaças de malware a fim de confirmar se tais sistemas continuam sendo considerados como não normalmente afetados por softwares mal-intencionados?	▪ Entreviste a equipe	☐	☐	☐	☐
5.2	Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue:					
	(a) Todos os softwares antivírus e as definições são mantidos atualizados?	▪ Examine as políticas e procedimentos ▪ Examine as configurações do antivírus, incluindo a instalação principal ▪ Examine os componentes do sistema	☐	☐	☐	☐
	(b) As atualizações automáticas e as varreduras periódicas estão ativadas e sendo executadas?	▪ Examine as configurações do antivírus, incluindo a instalação principal ▪ Examine os componentes do sistema	☐	☐	☐	☐
	(c) Todos os mecanismos antivírus geram logs de auditoria e os logs são mantidos de acordo com o Requisito 10.7 do PCI DSS?	▪ Examine as configurações do antivírus ▪ Reveja os processos de retenção de registro	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
5.3	Todos os mecanismos do antivírus: ▪ Estão sendo executados ativamente? ▪ Não podem ser desativados ou alterados pelos usuários? ***Observação:*** *as soluções antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período de tempo durante o qual a proteção antivírus não estiver ativa.*	▪ Examine as configurações do antivírus ▪ Examine os componentes do sistema ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐
5.4	Os procedimentos operacionais e as políticas de segurança para proteção dos sistemas contra malware são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas?	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.1	Há um processo para identificar vulnerabilidades de segurança, incluindo o seguinte: ▪ Uso de origens externas conhecidas para obter informações sobre vulnerabilidade? ▪ Classificação de uma escala de risco para as vulnerabilidades, o que inclui identificação de todas as vulnerabilidades de "alto risco" e "críticas"? ***Observação**: as classificações de risco devem ser baseadas nas melhores práticas do setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.* *Os métodos para avaliar as vulnerabilidades e classificar o nível de risco variam com base no ambiente da organização e na estratégia de avaliação de risco. As classificações de risco devem, no mínimo, identificar todas as vulnerabilidades consideradas de "alto risco" ao ambiente. Além da classificação de risco, as vulnerabilidades podem ser consideradas "críticas" se apresentarem uma ameaça iminente ao ambiente, sistemas críticos de impacto e/ou resultariam em comprometimento potencial se não resolvidas. Exemplos de sistemas críticos podem incluir sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão.*	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.2	(a) Todos os componentes e softwares do sistema estão protegidos de vulnerabilidades conhecidas devido à instalação de patches de segurança aplicáveis disponibilizados pelo fornecedor?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐
	(b) Os patches de segurança críticos são instalados no prazo de um mês após o lançamento? ***Observação**: os patches de segurança crítica devem ser identificados de acordo com o processo de classificação de risco definido no Requisito 6.1.*	▪ Reveja as políticas e procedimentos ▪ Examine os componentes do sistema ▪ Compare a lista de patches de segurança instalados com as listas de patches recentes do fornecedor	☐	☐	☐	☐
6.4.5	(a) São documentados os procedimentos de controle de alterações e requerem o seguinte? • Documentação de impacto • Aprovação de controle de alteração documentada pelas partes autorizadas • Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema • Procedimentos de reversão	▪ Reveja os procedimentos e processos de controle de alteração	☐	☐	☐	☐
	(b) Os seguintes itens são executados e documentados para todas as alterações:					
6.4.5.1	Documentação de impacto?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐
6.4.5.2	Aprovação documentada pelas partes autorizadas	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.4.5.3	(a) Teste a funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐
	(b) Para alterações do código personalizado, todas as atualizações foram testadas quanto à conformidade com o Requisito 6.5 do PCI DSS antes de serem implantadas na produção?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐
6.4.5.4	Procedimentos de back-out?	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração	☐	☐	☐	☐
6.4.6	Após a conclusão de uma mudança significativa, são implementados todos os requisitos do PCI DSS em todos os sistemas novos ou alterados e redes, e atualizada a documentação conforme aplicável? ***Observação:*** *este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.*	▪ Rastreie as alterações para alterar a documentação de controle ▪ Examine a documentação de controle de alteração ▪ Entreviste a equipe ▪ Observar os sistemas ou redes afetados	☐	☐	☐	☐
6.5	Os processos de desenvolvimento do software abordam vulnerabilidades de codificação comum?	▪ Reveja os procedimentos e políticas de desenvolvimento de software	☐	☐	☐	☐
	Os desenvolvedores são treinados pelo menos anualmente em técnicas de codificação seguras atualizadas, incluindo como evitar vulnerabilidades comuns de codificação?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Examine os registros de treinamento	☐	☐	☐	☐
	(c) Os aplicativos são desenvolvidos com base nas diretrizes de codificação segura para proteger aplicativos das seguintes vulnerabilidades, no mínimo:					

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.5.1	As técnicas de codificação direcionam defeitos de injeção, particularmente injeção SQL? ***Observação:*** *também considere as falhas de injeção OS Command Injection, LDAP e XPath, assim como outras falhas.*	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.2	As técnicas de codificação direcionam as vulnerabilidades de estouro de buffer?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.4	As técnicas de codificação abordam as comunicações não seguras?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.5	As técnicas de codificação abordam a manipulação incorreta de erros?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.6	As técnicas de codificação abordam todas as vulnerabilidades classificadas como de "alto risco" identificadas no processo de identificação de vulnerabilidade (conforme definido no Requisito 6.1 do PCI DSS)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
Para as interfaces de aplicativo e aplicativos da Web (internos ou externos), os aplicativos são desenvolvidos com base nas diretrizes de codificação segura para proteger os aplicativos das seguintes vulnerabilidades adicionais:						
6.5.7	As técnicas de codificação direcionam as vulnerabilidades de script entre sites (XSS)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.5.8	As técnicas de controle direcionam controle inadequado de acesso, como referências diretas não seguras a objetos, falhas em restringir o acesso a URLs, diretórios transversais e falhas em restringir o acesso do usuário às funções?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.9	As técnicas de codificação direcionam falsificação de solicitação entre sites (CSRF)?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐
6.5.10	As técnicas de codificação direcionam gerenciamento de sessão e autenticação inválida?	▪ Examine os procedimentos e políticas de desenvolvimento de software ▪ Entreviste a equipe responsável	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.6	Para aplicativos da Web voltados para o público, as novas ameaças e vulnerabilidades são abordadas continuamente e esses aplicativos estão protegidos contra ataques conhecidos por *qualquer* um dos métodos a seguir? ▪ Analisando os aplicativos da Web voltados para o público por meio de ferramentas ou métodos manuais ou automáticos de avaliação de segurança das vulnerabilidades dos aplicativos, conforme os itens a seguir: - Pelo menos uma vez ao ano - Após quaisquer alterações - Por meio de uma empresa especializada na segurança de aplicativos - Se, pelo menos, todas as vulnerabilidades no Requisito 6.5 estão incluídas na avaliação - Se todas as vulnerabilidades são corrigidas - Se o aplicativo for reavaliado após as correções ***Observação**: esta avaliação não é igual às varreduras de vulnerabilidades realizadas para o Requisito 11.2.* – **OU** – ▪ Instalar uma solução técnica automatizada que detecta e previne ataques baseados na web (por exemplo, um firewall de aplicativo da web) conforme a seguir: - Está situada diante de aplicativos da Web voltados ao público para detectar e prevenir invasões baseadas na Web. - Está funcionando ativamente e atualizada conforme aplicável. - Está gerando logs de auditoria. - Está configurado para bloquear ataques baseados na web, ou gerar um alerta que é imediatamente investigado.	▪ Reveja os processos documentados ▪ Entreviste a equipe ▪ Examine os registros de avaliações de segurança de aplicativo ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
6.7	Os procedimentos operacionais e as políticas de segurança para o desenvolvimento e manutenção dos aplicativos e sistemas seguros são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas?	▪ Reveja as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐

Implemente medidas rigorosas de controle de acesso

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

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

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
8.1	Há procedimentos e políticas para os controles de gerenciamento de identificação de administradores e usuários que não são clientes em todos os componentes do sistema, como segue:					
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	☐	☐	☐	☐
8.1.2	As adições, exclusões e modificações dos IDs, das credenciais e de outros objetos de identificação dos usuários são controladas de forma que os IDs dos usuários sejam implementados somente quando autorizados (incluindo usuários com privilégios específicos)?	▪ Reveja os procedimentos de senha ▪ Examine os IDs do usuário geral e privilegiado e as autorizações associadas ▪ Observe as definições do sistema				
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	☐	☐	☐	☐
8.1.4	As contas de usuários inativos são removidas ou desabilitadas no prazo de 90 dias?	▪ Reveja os procedimentos de senha ▪ Observe as contas do usuário	☐	☐	☐	☐
8.1.5	(a) As contas são usadas por terceiros para acessar, suportar ou manter componentes do sistema via acesso remoto habilitado somente durante o período necessário e desativado quando não estiver em uso?	▪ Reveja os procedimentos de senha ▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐
	(b) As contas de acesso remoto de terceiros são monitoradas quando em uso?	▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
8.1.6	(a) As tentativas de acesso repetidas são limitadas bloqueando o ID do usuário após seis tentativas, no máximo?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
8.1.7	Após o bloqueio da conta do usuário, a duração do bloqueio está definida para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
8.1.8	Se uma sessão ficar ociosa por mais de 15 minutos, o usuário é obrigado a se autenticar novamente (informar novamente a senha, por exemplo) para reativar o terminal ou a sessão?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
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	☐	☐	☐	☐
8.2.1	(a) É usada uma criptografia forte para processar todas as credenciais de autenticação (como senhas/frases secretas) de modo ilegível durante o transporte e armazenamento em todos os componentes do sistema?	▪ Reveja os procedimentos de senha ▪ Reveja a documentação do fornecedor ▪ Examine as definições de configuração do sistema ▪ Observe os arquivos de senha ▪ Observe as transmissões de dados	☐	☐	☐	☐
8.2.2	A identidade do usuário é identificada antes de modificar qualquer credencial de autenticação, por exemplo, executar restauração da senha, provisionar novos tokens ou gerar novas chaves?	▪ Reveja os procedimentos de autenticação ▪ Observe a equipe	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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	☐	☐	☐	☐
8.2.4	(a) As senhas de usuário/frases secretas são alteradas pelo menos uma vez a cada 90 dias?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
8.2.5	(a) Uma pessoa deve criar uma nova senha/frase secreta que seja diferente das últimas quatro senhas/frases secretas usadas?	▪ Reveja os procedimentos de senha ▪ Amostra de componentes do sistema ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐
8.2.6	As senhas/frases secretas são definidas com um valor exclusivo para cada usuário na primeira utilização e após reiniciar, e cada usuário deve mudar sua senha imediatamente após o primeiro uso?	▪ Reveja os procedimentos de senha ▪ Examine as definições de configuração do sistema ▪ Observe a equipe de segurança	☐	☐	☐	☐
8.3	Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE é protegido usando a autenticação multifatores, conforme a seguir? ***Observação:*** *a autenticação multifatores exige que um mínimo de dois dos três métodos de autenticação (ver Exigência 8.2 de PCI DSS para obter descrições dos métodos de autenticação) seja usado para autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifatores.*					

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
8.3.1	É incorporada autenticação multifatores em todos os acessos que não utilizam console no CDE para os funcionários com acesso administrativo? ***Observação:*** *este requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se uma exigência.*	▪ Examine as configurações do sistema ▪ Observar o login de administrador no CDE	☐	☐	☐	☐
8.3.2	É incorporada autenticação multifatores em todos os acessos de rede remota (usuário e administrador e incluindo o acesso de terceiros para suporte ou manutenção) provenientes de fora da rede da entidade?	▪ Examine as configurações do sistema ▪ Observar os funcionários se conectando remotamente	☐	☐	☐	☐
8.4	(a) Os procedimentos e políticas de autenticação são documentados e comunicados a todos os usuários?	▪ Reveja as políticas e procedimentos ▪ Reveja o método de distribuição ▪ Entreviste a equipe ▪ Entreviste os usuários	☐	☐	☐	☐
	(b) Os procedimentos e políticas de autenticação incluem o seguinte? • Orientação sobre selecionar credenciais fortes de autenticação • Orientação sobre como os usuários devem proteger suas credenciais de autenticação • Instruções para não reutilizar senhas anteriormente usadas • Instruções para os usuários de alteração da senha se houver suspeita de que ela possa estar comprometida	▪ Reveja as políticas e procedimentos ▪ Reveja a documentação fornecida aos usuários	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
8.5	As contas e senhas (ou outros métodos de autenticação) de grupo, compartilhadas ou genéricas, são proibidas conforme os itens a seguir: ▪ Os IDs e as contas de usuários genéricos são desativados ou removidos; ▪ Não existem IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas; e ▪ 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	☐	☐	☐	☐
8.6	Onde forem usados outros mecanismos de autenticação (por exemplo, tokens de segurança físicos ou lógicos, cartões inteligentes, certificados, etc.), o uso destes mecanismos é atribuído como segue? ▪ Os mecanismos de autenticação devem ser atribuídos a uma conta individual e não compartilhados entre várias contas ▪ Controles físicos e/ou lógicos devem ser implementados para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso	▪ Reveja as políticas e procedimentos ▪ Entreviste a equipe ▪ Examine as definições da configuração do sistema e/ou controles físicos	☐	☐	☐	☐
8.8	Os procedimentos operacionais e políticas de segurança para a identificação e autenticação são/estão: ▪ Documentados ▪ Em uso ▪ Conhecidos por todas as partes envolvidas?	▪ Examine as políticas de segurança e procedimentos operacionais ▪ Entreviste a equipe	☐	☐	☐	☐

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

	Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
9.1	Existem controles adequados em vigor para a entrada na instalação, de forma a limitar e monitorar o acesso físico aos sistemas no ambiente de dados do titular do cartão?	▪ Observe os controles de acesso físico ▪ Observe a equipe	☐	☐	☐	☐
9.5	Todas as mídias estão fisicamente seguras (incluindo, entre outros, computadores, mídias eletrônicas removíveis, recibos em papel, relatórios em papel e faxes)? *Para os fins do requisito 9, "mídia" refere-se a todas as mídias em papel ou eletrônicas que contêm dados do titular do cartão.*	▪ Reveja as políticas e procedimentos para segurança física das mídias ▪ Entreviste a equipe	☐	☐	☐	☐
9.6	(a) É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia?	▪ Reveja as políticas e procedimentos para distribuição de mídia	☐	☐	☐	☐
	(b) Os controles incluem o seguinte:					
9.6.1	A mídia é classificada para que a confidencialidade dos dados possa ser determinada?	▪ Reveja as políticas e procedimentos para classificação de mídia ▪ Entreviste a equipe de segurança	☐	☐	☐	☐
9.6.2	A mídia é enviada via um mensageiro seguro ou outro método de entrega que possa ser rastreado com precisão?	▪ Entreviste a equipe ▪ Examine a documentação e registros de rastreamento da distribuição de mídia	☐	☐	☐	☐
9.6.3	A aprovação gerencial é obtida antes de mover as mídias (especialmente quando a mídia é distribuída a pessoas)?	▪ Entreviste a equipe ▪ Examine a documentação e registros de rastreamento da distribuição de mídia	☐	☐	☐	☐
9.7	É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias?	▪ Reveja as políticas e procedimentos	☐	☐	☐	☐

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

Monitorar e testar as redes regularmente

Requisito 10: Acompanhe e monitore todos os acessos com relação aos recursos da rede e aos dados do titular do cartão

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.1	Trilhas de auditoria estão habilitadas e ativas para os componentes do sistema?	▪ Observe os processos ▪ Entreviste o administrador do sistema	☐	☐	☐	☐
	O acesso aos componentes do sistema está ligado aos usuários individuais?	▪ Observe os processos ▪ Entreviste o administrador do sistema	☐	☐	☐	☐
10.2	Foram implementadas trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:					
10.2.2	Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.2.3	Acesso a todas as trilhas de auditoria?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.2.4	Tentativas de acesso lógico inválidas?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.2.5	Há uso e alterações dos mecanismos de identificação e autenticação, incluindo, entre outros, a criação de novas contas e aumento de privilégios e todas as alterações, adições ou exclusões de contas com privilégios raiz ou administrativos?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.2.6	Inicialização, interrupção ou pausa dos registros de auditoria?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.2.7	Criação e exclusão de objetos em nível de sistema?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.3	As seguintes entradas da trilha de auditoria são registradas para todos os componentes do sistema em cada um dos eventos a seguir?					
10.3.1	Identificação do usuário?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.3.2	Tipo de evento?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.3.3	Data e hora?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.3.4	Indicação de sucesso ou falha?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.3.5	Origem do evento?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.3.6	Identidade ou nome dos dados, componentes do sistema ou recursos afetados?	▪ Entreviste a equipe ▪ Observe os logs de auditoria ▪ Examine as definições do log de auditoria	☐	☐	☐	☐
10.4	Todos os relógios e horários dos sistemas críticos estão sincronizados por meio do uso de uma tecnologia de sincronização e essa tecnologia é mantida atualizada? ***Observação:*** *um exemplo de tecnologia de sincronização de horários é o Network Time Protocol (NTP).*	▪ Reveja os processos e padrões de configuração de horário	☐	☐	☐	☐
10.4.1	Os seguintes processos são implementados nos sistemas críticos para obter um horário consistente e correto:					
	(a) Apenas os servidores centrais designados recebem sinais de tempo de fontes externas, e os sinais de tempo de fontes externas são baseados no tempo atômico internacional ou UTC?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐
	(b) Onde há mais de um servidor de tempo designado, os servidores de horário se comunicam para manter o horário exato?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐
	(c) Os sistemas recebem o horário apenas de servidores centrais designados?	▪ Reveja os processos e padrões de configuração de horário ▪ Examine os parâmetros do sistema relacionados ao horário	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.4.2	Os dados de horário são protegidos conforme a descrição a seguir? (a) O acesso aos dados de horário é restrito somente às equipes com necessidades profissionais de acessá-los?	▪ Examine as configurações do sistema e as definições de sincronização de horário	☐	☐	☐	☐
	(b) As alterações nas configurações de horários dos sistemas críticos são registradas, monitoradas e analisadas?	▪ Examine as configurações do sistema e os registros e configurações de sincronização de horário	☐	☐	☐	☐
10.4.3	As configurações de horário são recebidas de fontes de horário específicas aceitas pelo setor (isso é feito para evitar a alteração do relógio por um indivíduo mal-intencionado)? *Além disso, essas atualizações podem ser criptografadas com uma chave simétrica e as listas de controle de acesso podem ser criadas para especificar os endereços IP das máquinas clientes que serão fornecidas com as atualizações de horário (para evitar o uso não autorizado de servidores de horário internos).*	▪ Examine as configurações do sistema	☐	☐	☐	☐
10.5	As trilhas de auditoria estão protegidas de forma que não possam ser alteradas, conforme a descrição a seguir?					
10.5.1	A visualização das trilhas de auditoria é limitada às pessoas com necessidades relacionadas à função?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐
10.5.2	Os arquivos de trilha de auditoria estão protegidos contra modificações não autorizadas por meio de mecanismos de controle de acesso, separação física e/ou separação da rede?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.5.3	O backup dos arquivos de trilha de auditoria é feito imediatamente em um servidor de log centralizado ou em uma mídia que seja difícil de alterar?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐
10.5.4	Os logs para tecnologias externas (por exemplo, sem fio, firewalls, DNS, e-mail) são escritos em um servidor ou mídia de registro interno, centralizado e seguro?	▪ Entreviste os administradores do sistema ▪ Examine as permissões e configurações do sistema	☐	☐	☐	☐
10.5.5	São usados softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos logs para assegurar que os dados do log existentes não possam ser alterados sem gerar alertas (embora os novos dados que estejam sendo adicionados não gerem um alerta)?	▪ Examine as definições, arquivos monitorados e resultados das atividades de monitoramento	☐	☐	☐	☐
10.6	Os logs e ocorrências de segurança para todos os componentes do sistema são revisados para identificar irregularidades ou atividades suspeitas como segue? ***Observação:*** *as ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6*					

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
10.6.1	(b) Os seguintes logs e ocorrências de segurança são revisados, no mínimo, diariamente, de modo manual ou por ferramentas de log? • Todas as ocorrências de segurança • Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD • Logs de todos os componentes críticos do sistema • Logs de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do comércio eletrônico, etc.)	▪ Reveja os procedimentos e políticas de segurança ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐
10.6.2	(b) Os logs de todos os outros componentes do sistema são revisados periodicamente, de modo manual ou por ferramentas de log, com base na estratégia de gerenciamento de risco e nas políticas da organização?	▪ Reveja os procedimentos e políticas de segurança ▪ Reveja a documentação de avaliação de risco ▪ Entreviste a equipe	☐	☐	☐	☐
10.6.3	(b) Há um acompanhamento das exceções e irregularidades identificadas durante o processo de revisão?	▪ Reveja os procedimentos e políticas de segurança ▪ Observe os processos ▪ Entreviste a equipe	☐	☐	☐	☐
10.7	(b) Os logs de auditoria são retidos pelo menos uma vez ao ano?	▪ Reveja os procedimentos e políticas de segurança ▪ Entreviste a equipe ▪ Examine os logs de auditoria	☐	☐	☐	☐
	(c) Ao menos os últimos três meses de logs estão imediatamente disponíveis para análise?	▪ Entreviste a equipe ▪ Observe os processos	☐	☐	☐	☐

Requisito 11: Testar regularmente os sistemas e processos de segurança

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
11.2.2	(a) As varreduras das vulnerabilidades externas são executadas trimestralmente? ***Observação:*** *as varreduras externas trimestrais de vulnerabilidades devem ser realizadas por um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da indústria de cartões de pagamento (PCI SSC).* *Consulte o Guia do programa ASV publicado no site do PCI SSC para saber sobre responsabilidades de varredura do cliente, preparação de varredura, etc.*	▪ Reveja os resultados dos quatro últimos trimestres quanto às varreduras de vulnerabilidades externas	☐	☐	☐	☐
	(b) Os resultados da varredura externa trimestral cumprem os requisitos do *Guia do programa ASV* (por exemplo, nenhuma vulnerabilidade classificada com valor 4 ou superior pelo CVSS e nenhuma falha automática)?	▪ Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente	☐	☐	☐	☐
	(c) As varreduras de vulnerabilidades externas trimestrais são executadas por um fornecedor de varredura aprovado (ASV) pela PCI SSC?	▪ Reveja os resultados de cada varredura e nova varredura externas feitas trimestralmente	☐	☐	☐	☐
11.2.3	(a) Varreduras internas e externas e novas varreduras são realizadas, se necessário, após qualquer mudança significativa? ***Observação:*** *as varreduras devem ser realizadas por uma equipe qualificada.*	▪ Examine e correlacione a documentação de controle de alteração e os relatórios de varredura	☐	☐	☐	☐
	(b) O processo de varredura inclui novas varreduras até que: • Não existam varreduras com pontuação de 4 ou mais pelo CVSS para varreduras externas; • Um resultado aprovado seja obtido ou todas as vulnerabilidades definidas como "alto risco", conforme definido no Requisito 6.1 do PCI DSS, estejam solucionadas (para varreduras internas)?	▪ Reveja os relatórios de varredura	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(c) As varreduras são executadas por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	▪ Entreviste a equipe	☐	☐	☐	☐
11.3	A metodologia de teste de penetração inclui o seguinte? ▪ É baseada nas abordagens de testes de penetração aceitas pelo setor (por exemplo, NIST SP800-115) ▪ Abrange todo o perímetro do CDE e sistemas críticos ▪ Inclui testes de dentro e fora da rede ▪ Inclui testes para validar qualquer controle de redução no escopo e segmentação ▪ Define testes de penetração da camada do aplicativo para incluir, pelo menos, as vulnerabilidades listadas no requisito 6.5 ▪ Define testes de penetração da camada da rede que incluam componentes compatíveis com as funções da rede e com os sistemas operacionais ▪ Inclui revisão e consideração de ameaças e vulnerabilidades ocorridas nos últimos 12 meses ▪ Especifica a retenção dos resultados de testes de penetração e resultados de atividades de reparo	▪ Examine a metodologia de teste de penetração ▪ Entreviste a equipe responsável	☐	☐	☐	☐
11.3.1	(a) É realizado um teste de penetração *externo* pela metodologia definida, pelo menos anualmente e após qualquer alteração significativa de infraestrutura ou aplicativo no ambiente (como uma atualização do sistema operacional, uma adição de sub-rede no ambiente, ou um servidor da web adicionado)?	▪ Examine o escopo do trabalho ▪ Examine os resultados do teste mais recente de penetração externa	☐	☐	☐	☐
	(b) São realizados testes por um recurso interno qualificado ou terceiro externo qualificado e, se for o caso, existe a independência organizacional do testador (não é requerido ser um QSA ou ASV)?	▪ Entreviste a equipe responsável	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
11.3.3	As vulnerabilidades exploráveis encontradas durante o teste de penetração são corrigidas e o teste é repetido para verificar as correções?	▪ Examine os resultados do teste de penetração	☐	☐	☐	☐
11.3.4	Se a segmentação é usada para isolar o CDE de outras redes:					
	(a) São definidos procedimentos de teste de penetração para testar todos os métodos de segmentação, para confirmar que eles estão operacionais e eficientes e que isolam-se todos os sistemas fora de escopo dos sistemas no CDE?	▪ Examine os controles de segmentação ▪ Reveja a metodologia de teste de penetração	☐	☐	☐	☐
	(b) O teste de penetração para verificar os controles de segmentação atende ao seguinte? • É executado pelo menos uma vez ao ano e após qualquer mudança nos métodos/controles da segmentação • Abrange todos os métodos/controles da segmentação em uso • Verifica se os métodos de segmentação estão operacionais e eficientes e isola todos os sistemas fora de escopo dos sistemas no CDE	▪ Examine os resultados do teste mais recente de penetração	☐	☐	☐	☐
	(c) São realizados testes por um recurso interno qualificado ou terceiro externo qualificado e, se for o caso, existe a independência organizacional do testador (não é requerido ser um QSA ou ASV)?	▪ Entreviste a equipe responsável	☐	☐	☐	☐

	Pergunta do PCI DSS	Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/D**
11.4	(a) As técnicas de prevenção contra intrusão e/ou detecção de intrusão que detectam e/ou evitam instruções na rede estão em uso para monitorar todo o tráfego: • No perímetro do ambiente dos dados do titular do cartão, e • Nos pontos críticos do ambiente dos dados do titular do cartão.	▪ Examine as configurações do sistema ▪ Examine os diagramas da rede	☐	☐	☐	☐
	(b) As técnicas de prevenção contra intrusão e/ou detecção de intrusão estão configuradas para alertar a equipe sobre comprometimentos suspeitos?	▪ Examine as configurações do sistema ▪ Entreviste a equipe responsável	☐	☐	☐	☐
	(c) Todos os mecanismos, diretrizes e assinaturas para detecção e prevenção contra invasões estão atualizados?	▪ Examine as configurações de IDS/IPS ▪ Examine a documentação do fornecedor	☐	☐	☐	☐
11.5	(a) Existe um mecanismo de detecção de mudança (por exemplo, ferramentas de monitoramento de integridade de arquivo) implementado para detectar modificações não autorizadas (incluindo as alterações, adições e exclusões) de arquivos críticos de sistema, arquivos de configuração ou arquivos de conteúdo? *Os exemplos de arquivos que devem ser monitorados incluem:* • *Executáveis do sistema* • *Executáveis dos aplicativos* • *Arquivos de configuração e parâmetro* • *Arquivos de log e auditoria, históricos ou arquivados, armazenados centralmente* • *Arquivos críticos adicionais determinados pela entidade (por exemplo, por meio de avaliação de risco ou outros meios)*	▪ Observe as definições do sistema e os arquivos monitorados ▪ Examine as definições de configuração do sistema	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
	(b) O mecanismo de detecção de mudança é configurado para alertar os funcionários sobre modificação não autorizada (incluindo as alterações, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo, e as ferramentas realizam comparações de arquivos críticos pelo menos semanalmente? ***Observação:*** *para fins de detecção de alterações, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Os mecanismos de detecção de alterações, como produtos de monitoramento da integridade dos arquivos, normalmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para os aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).*	▪ Observe as definições do sistema e os arquivos monitorados ▪ Reveja os resultados das atividades de monitoramento	☐	☐	☐	☐
11.5.1	Há um processo implementado para responder a qualquer alerta gerado pela solução de detecção de alterações?	▪ Examine as definições de configuração do sistema	☐	☐	☐	☐

Manter uma política de segurança de informações

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

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada para todas as equipes relevantes?	▪ Reveja a política de segurança de informações	☐	☐	☐	☐
12.1.1	A política de segurança é revisada ao menos uma vez por ano e atualizada quando o ambiente é alterado?	▪ Reveja a política de segurança de informações ▪ Entreviste a equipe responsável	☐	☐	☐	☐
12.4	A política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todas as equipes?	▪ Reveja os procedimentos e a política de segurança ▪ Entreviste alguns dos funcionários responsáveis	☐	☐	☐	☐
12.5	(b) As seguintes responsabilidades do gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e para as equipes que:					
12.5.3	Estabelecem, documentam e distribuem procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?	▪ Reveja os procedimentos e a política de segurança	☐	☐	☐	☐
12.6	(a) Existe um programa de conscientização de segurança formal para tornar todos os funcionários conscientes da política e dos procedimentos de segurança dos dados dos titulares de cartão?	▪ Reveja o programa de conscientização de segurança	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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 eles possuem do titular do cartão, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente? ***Observação:*** *as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.*	▪ Observe os acordos por escrito ▪ Reveja as políticas e procedimentos	☐	☐	☐	☐
12.8.3	Existe um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐
12.8.4	É mantido um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐
12.8.5	As informações mantidas sobre os requisitos do PCI DSS são administradas por cada prestador de serviços e quais são administradas pela entidade?	▪ Observe os processos ▪ Reveja as políticas e procedimentos e os documentos de suporte	☐	☐	☐	☐

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	Sim com CCW	Não	N/D
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	☐	☐	☐	☐
	(b) No mínimo, o plano aborda o seguinte:					
	• Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo, no mínimo, a notificação às bandeiras?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Procedimentos de resposta específicos a incidentes?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Procedimentos de recuperação e continuidade dos negócios?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Processos de backup dos dados?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Análise dos requisitos legais para divulgação dos comprometimentos?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Abrangência e respostas de todos os componentes críticos do sistema?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐
	• Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras?	▪ Reveja os procedimentos do plano de resposta a incidentes	☐	☐	☐	☐

Apêndice A: Requisitos adicionais do PCI DSS

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

Esse apêndice não é usado para avaliações de comerciante.

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

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

Pergunta do PCI DSS		Teste esperado	Resposta *(Marque uma resposta para cada pergunta)*			
			Sim	**Sim com CCW**	**Não**	**N/D**
A2.2	Existe um plano formal de redução de riscos e migração em vigor para todas as implementações que usam SSL ou TLS precoce (exceto conforme permitido em A2.1), que inclui: ▪ Descrição de uso, incluindo dados que estão sendo transmitidos, tipos e número de sistemas que usam e/ou suporte SSL/TLS precoce, tipo de ambiente; ▪ Resultados da avaliação de riscos e controles de redução de risco no lugar; ▪ Descrição dos processos para monitorar as novas vulnerabilidades associadas com SSL/TLS precoce; ▪ Descrição de processos de controle de alterações que são implementados para garantir que a SSL/TLS precoce não seja implementada em novos ambientes; ▪ Visão geral do plano do projeto de migração, incluindo a data de conclusão do objetivo da migração até no máximo 30 de junho de 2018?	▪ Rever plano de redução de riscos e migração documentado	☐	☐	☐	☐

Anexo A3: Validação Suplementar de Entidades Designadas (DESV)

Este anexo se aplica apenas a entidades designadas por uma empresa de pagamento ou adquirente que exigem uma validação adicional dos requisitos existentes do PCI DSS. Entidades que precisam validar esse apêndice devem usar o modelo de relatório suplementar DESV e atestado suplementar de conformidade para relatórios e consultar a empresa de pagamento e/ou adquirente aplicável sobre os procedimentos de envio.

Apêndice B: Planilha dos controles de compensação

Use essa planilha para definir os controles de compensação para requisitos em que "SIM com CCW" foi selecionado.

Observação: *somente as empresas que realizaram uma análise dos riscos e têm restrições de negócios documentadas ou tecnológicas legítimas podem considerar o uso dos controles de compensação para atingir a conformidade.*

Consulte os Apêndices B, C e D do PCI DSS para obter informações sobre os controles de compensação e orientação sobre como preencher essa planilha.

Número e definição do requisito:

	Informações necessárias	Explicação
1. Restrições	Liste as restrições que impossibilitam a conformidade com o requisito original.	
2. Objetivo	Defina o objetivo do controle original; identifique o objetivo atendido pelo controle de compensação.	
3. Risco identificado	Identifique qualquer risco adicional imposto pela ausência do controle original.	
4. Definição dos controles de compensação	Defina os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	
5. Validação dos controles de compensação	Defina como os controles de compensação foram validados e testados.	
6. Manutenção	Defina o processo e os controles implementados para manter os controles de compensação.	

Apêndice C: Explicação de não aplicabilidade

Se a coluna "N/D" (não disponível) tiver sido selecionada no questionário, use esta planilha para explicar por que o requisito relacionado não se aplica à sua organização.

Requisito	Motivo pelo qual o requisito não se aplica
Exemplo:	
3.4	Os dados do titular do cartão nunca são armazenados eletronicamente

Seção 3: Detalhes de atestado e validação

Parte 3. Validação do PCI DSS

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

Baseado nos resultados documentados no SAQ A-EP observado acima, os signatários identificados nas Partes 3b-3d, conforme aplicável afirmam o seguinte estado de conformidade para a entidade identificada na Parte 2 deste documento: (***selecione um):***

☐	**Em conformidade:** todas as seções do SAQ do PCI DSS estão preenchidas e todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **CONFORMIDADE**, de forma que a *(nome da empresa do comerciante)* demonstrou conformidade integral com o PCI DSS.
☐	**Não conformidade:** nem todas as seções do SAQ do PCI DSS estão preenchidas ou nem todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **NÃO CONFORMIDADE**, de forma que a *(nome da empresa do comerciante)* não demonstrou conformidade integral com o PCI DSS. **Data prevista** para conformidade: A entidade que estiver enviando este formulário com um status de Não conformidade talvez tenha de preencher o Plano de ação na Parte 4 deste documento. *Verifique junto ao seu adquirente ou à(s) empresa(s) de pagamento antes de preencher a Parte 4.*
☐	**Em conformidade, mas com exceção legal:** um ou mais dos requisitos foram marcados como "não" devido a uma restrição legal que evita que o requisito seja atendido. Essa opção exige revisão adicional do adquirente ou empresa de pagamento. *Se selecionada, preencha o seguinte:*

Requisito afetado	Detalhes de como a restrição legal evita que o requisito seja atendido

Parte 3a. Reconhecimento do status

O(s) signatário(s) confirma(m):

(Selecione todos os aplicáveis)

☐	O Questionário de autoavaliação A-EP 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 representante devidamente autorizado da empresa do 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 portador do cartão e a data de vencimento.

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

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

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

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

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

Exigência do PCI DSS*	Descrição do requisito	Em conformidade com os requisitos do PCI DSS (selecione um)		Data de reparação e ações (se "NÃO" estiver selecionado para qualquer requisito)
		SIM	NÃO	
1	Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão	☐	☐	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐	☐	
3	Proteger os dados armazenados do titular do cartão	☐	☐	
4	Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas	☐	☐	
5	Proteger 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 titular do cartão de acordo com a necessidade de conhecimento para o negócio	☐	☐	
8	Identificar e autenticar o acesso aos componentes do sistema	☐	☐	
9	Restringir o acesso físico aos dados do titular do cartão	☐	☐	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão	☐	☐	
11	Testar regularmente os sistemas e processos de segurança	☐	☐	
12	Manter uma política que aborde a segurança da informação para todas as equipes	☐	☐	
Anexo A2	Requisitos adicionais de PCI DSS para entidades que usam SSL/TLS precoce	☐	☐	

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