Indústria de cartões de pagamento (PCI)

Segurança em transações com PIN (PTS)

Guia do Programa de teste e aprovação do dispositivo

Versão 1.9

Junho de 2020

Alterações no documento

Data	Versão	Descrição
Setembro de 2010	1.0	Versão Inicial
Outubro de 2011	1.1	Adicionar classes de aprovação para criptografar leitores de cartões e não PEDS.
Julho de 2015	1.2	Foram adicionadas HSM v2 e esclarecimentos sobre taxas, classes de aprovação e datas de validade.
Setembro de 2013	1.3	Atualizado para POI v4 e esclarecimento para Integração, Protocolos Abertos, SRED, arquivamento de dispositivos, determinação do status da aprovação, avaliações delta, prazos de envio, taxas, leitores de cartões seguros e diferentes de PEDS.
Março de 2014	1.4	Foram feitas alterações nos requisitos de amostra do dispositivo. Foram feitas inclusões para comprometer o processo de notificação. Nova categoria de dispositivo definida —*Dispositivos com aprovação expirada.* Esclarecimentos adicionais fornecidos para os recursos da Classe de Aprovação — Compatibilidade com PIN, Gerenciamento de chaves e funções fornecidas. Definições atualizadas para dispositivos diferentes de PEDS e SCRs. Mais explicações apresentadas sobre o processo de avaliação delta.
2015	1.5	Processo modificado para solicitar a alteração do nome/endereço/detalhes de contato do negócio por meio de um Formulário de Solicitação de Alteração Administrativa enviado ao laboratório; alteração no ciclo de faturas; faturas rateadas emitidas em 1º de novembro para todos os dispositivos listados entre 2 de maio a 31 de outubro. Novas orientações sobre licenciamento (re-branding) do dispositivo de outro fornecedor.
2016	1.6	Atualizado para POI v5 e HSM v3. Prazos de teste reformulados. Novas informações adicionadas da classe de aprovação HSM para dispositivos de carregamento de chaves e plataformas de administração remota. Esclarecimentos para tipos de produto para produtos OEM independentes.
Maio de 2017	1.7	Requisito para modificação da política de segurança para alterações administrativas adicionado. O texto adicionado para alertar onde ISO PIN Block Format 4 é usado para criptografia PIN, especificamente AES, e o método em que é usado, ou seja, DUKPT, Fixo ou Chave mestre/de sessão. Apêndice B atualizado para POI v5.
Março de 2018	1.8	Classe de aprovação SCRP adicionada, inclusive especificações somente de SCRP para novas aprovações e datas de validade. Requisito para Atestado de Validação anual sobre alterações de firmware (Seção 3) adicionado. Alterações nos testes de canal lateral. Adicionado Apêndice D: Atestado de Validação PTS. Errata.

Data	Versão	Descrição
Junho de 2020	1.9	As dúvidas técnicas frequentes relacionadas com o programa foram migradas; o apêndice D foi atualizado, “Atestado de Validação PTS”; Apêndice E acrescentado, “Atestado de Dispositivos PTS”; Questionário do Fornecedor eliminado; errata.

TERMO DE RECONHECIMENTO: A versão em inglês deste documento, conforme disponibilizada no site da PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês,a versão em inglês disponibilizada no local mencionado prevalecerá.

Sumário

1 Introdução

As seções a seguir apresentam informações básicas para este *Guia do programa de testes e aprovação de segurança em transações com PIN da PCI.*

1.1 Publicações relacionadas

Além deste Guia do Programa (que descreve o processo de teste e aprovação), a estrutura de segurança em transações com PIN (PTS) do Conselho de Padrões de Segurança (SSC) da Indústria de cartões de pagamento (PCI) envolve os seguintes documentos:

Observação: *Estes documentos são rotineiramente atualizados e afirmados novamente. As versões atuais devem ser consultadas na utilização desses requisitos. Os padrões mais atuais ficarão disponíveis em www.pcisecuritystandards.org.*

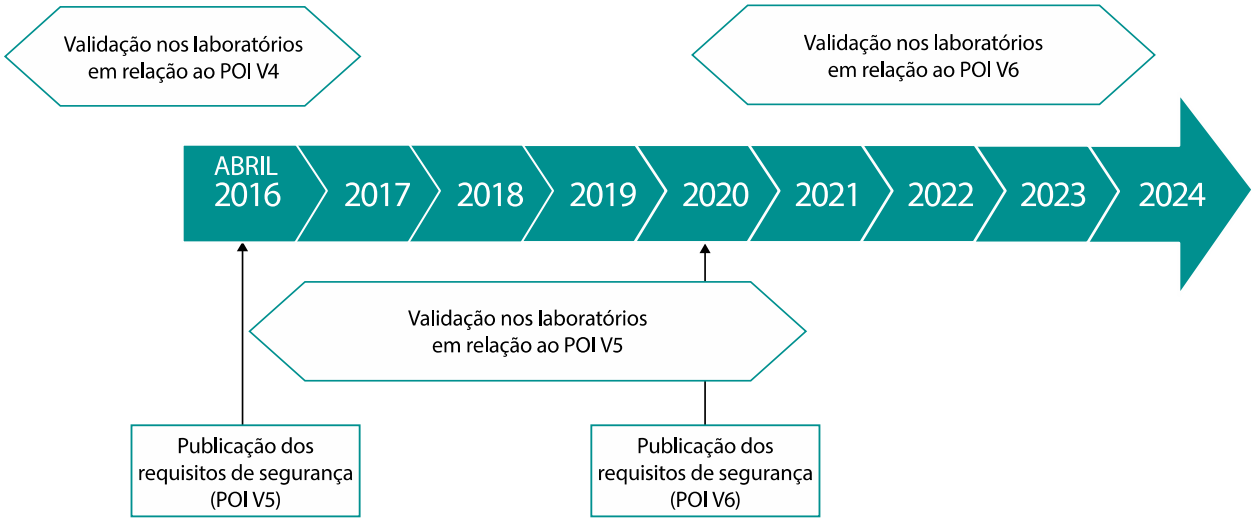
Nome do documento	Descrição
Requisitos de segurança	
▪ *Requisitos de segurança modular do ponto de interação (POI) da segurança em transações com PIN (PTS), v6.0* ▪ *Requisitos de Segurança do Módulo de Segurança de Hardware (HSM) para a Segurança de Transações com PIN (PTS), v3.0* ▪ *Procedimentos de teste e requisitos de segurança de PIN, v3.0*	O POI e o HSM contêm os requisitos físicos e lógicos do dispositivo de segurança, bem como os requisitos de gerenciamento de dispositivos para atividades antes do carregamento inicial da chave. Fornecer os formulários a serem utilizados por laboratórios e fornecedores. O PIN contém um conjunto completo de requisitos para a gestão segura, processamento e transmissão de dados de número de identificação pessoal (PIN) durante o processamento de transações de cartão de pagamento online e offline em caixas eletrônicos e terminais de ponto de venda (POS) atendidos e autônomos.
Dúvidas frequentes (FAQs)	
▪ *POI de PTS: Dúvidas frequentes*	Dúvidas gerais mais comuns
▪ *Perguntas téncias frequentes sobre requisitos de segurança de POI de PTS para uso com a Versão 6* ▪ *Dúvidas técnicas frequentes sobre os requisitos de segurança de PIN de PTS para uso com a Versão 3* ▪ *Dúvidas técnicas frequentes sobre o módulo de segurança de hardware (HSM) para uso com a Versão 3*	Apresentar esclarecimentos adicionais e em tempo oportuno para a aplicação dos Requisitos de segurança. As Dúvidas Frequentes fazem parte integrante desses requisitos e devem ser plenamente consideradas durante o processo de avaliação.

Nome do documento	Descrição
Questionário de avaliação de fornecedor	
▪ *Questionário de avaliação de fornecedor dos Módulos de Segurança de Hardware (HSM) para a Segurança de Transações com PIN (PTS), v3.0*	Solicite informações adicionais dos fornecedores para apoiar suas solicitações sobre a conformidade de seus dispositivos com esses requisitos.
Requisitos de teste derivados	
▪ *Requisitos de testes derivados do ponto de interação (POI) da segurança em transações com PIN (PTS), v6.0* ▪ *Requisitos de teste derivado do Módulo de Segurança de Hardware (HSM) para a Segurança de Transações com PIN (PTS), v3.0*	Apresentar orientação específica aos fornecedores sobre os métodos que os laboratórios de ensaio podem aplicar ao testar de acordo com os requisitos.
Lista de laboratórios reconhecidos	
▪ *Laboratórios reconhecidos pela Indústria de cartões de pagamento (PCI)*	Laboratórios reconhecidos atualmente para testes de dispositivos PTS.
Contrato de liberação do fornecedor	
▪ *Contrato de liberação do fornecedor da Indústria de cartões de pagamento*	Contém os termos e condições que regem a troca de informações entre os fornecedores e o PCI SSC.
Lista de modelos de terminais aprovados	
▪ *Dispositivos de segurança de transações com PIN aprovados*	Lista de dispositivos de segurança de transações com PIN aprovados pelo PCI SSC.

Os documentos descritos acima estão disponíveis na seção “Segurança de transações com PIN” do site do PCI SSC, em www.pcisecuritystandards.org. As versões anteriores dos documentos disponíveis encontram-se no arquivo de documentos de segurança de transação com PIN no mesmo site.

1.2 Atualizações de documentos e requisitos de segurança

A segurança é uma corrida constante contra atacantes em potencial. Consequentemente, é preciso revisar, atualizar e melhorar regularmente os requisitos de segurança empregados para avaliar os dispositivos de POI e os módulos de segurança de hardware, chamados coletivamente de “dispositivos de segurança de pagamento”. Dessa forma, o PCI SSC concordou que todos os requisitos de segurança envolvidos e os requisitos de teste associados serão atualizados normalmente a cada três anos. O diagrama que segue descreve o ciclo de três anos dos Requisitos de Segurança v5, seus antecessores e o sucessor v6.



O PCI SSC se reserva o direito de alterar, corrigir ou retirar requisitos de segurança a qualquer momento. Se tal alteração for necessária, o PCI SSC se esforçará para trabalhar em estreita colaboração com clientes[1] e fornecedores para ajudar a reduzir o impacto de quaisquer alterações.

[1] Clientes são instituições financeiras que:

a) Oferecem cartões de pagamento para uma ou mais marcas de pagamento participantes (emitentes);

b) Aceitam tais cartões de pagamento para desembolso em dinheiro e inserem o recibo de transação resultante direta ou indiretamente no intercâmbio (adquirentes); ou

c) Oferecem serviços financeiros a comerciantes ou terceiros autorizados que aceitam tais cartões de pagamento para mercadorias, serviços ou desembolso em dinheiro e, direta ou indiretamente, inserem o recibo da transação resultante no intercâmbio (adquirentes).

De acordo com quaisquer mandatos emitidos pelas marcas de pagamento participantes, os clientes devem utilizar os resultados de testes e aprovação da PCI SSC ao tomarem decisões sobre a compra de dispositivos que foram aprovados dentro da estrutura PCI PTS.

1.3 Sobre este documento

O *Guia do programa de testes e aprovação de dispositivos de segurança em transações com PIN da Indústria de cartões de pagamento (PTS)* disponibiliza informações aos fornecedores sobre o processo de avaliação e aprovação pelo PCI SSC de dispositivos de segurança de pagamento e reflete o alinhamento das marcas de pagamento com cartão participantes com um conjunto padrão de:

- Requisitos de segurança do ponto de interação (POI) e do módulo de segurança de hardware (HSM),
- Metodologias de teste e
- Processos de aprovação.

Neste documento:

- "Participantes da PCI" ou "Participantes de bandeira de pagamento da PCI" significa qualquer entidade atualmente admitida como membro do Conselho de acordo com a Lei de Empresa de Responsabilidade Limitada de Delaware.
  Os participantes da PCI a partir da data deste documento são American Express Travel Related Services Company, Inc., DFS Services LLC (Discover), JCB Advanced Technologies, Inc., MasterCard International Incorporated e Visa Holdings, Inc.
- "PCI SSC", "PCI" ou "Conselho" referem-se ao PCI Security Standards Council, LLC, empresa de responsabilidade limitada de Delaware, que consiste nas marcas de cartões de pagamento mencionadas acima em "participantes da PCI".
- "Dispositivos de ponto de interação (POI)" refere-se em temos gerais a todos os dispositivos que aceitam PIN usados em transações em contato com o consumidor. Outros tipos de dispositivos em contato com o consumidor, conforme descrito no Apêndice A, podem ser incluídos na estrutura de POI, para lidar com todas as ameaças emergentes aos dados confidenciais dos participantes da PCI ou de titulares do cartões.
- "Módulos de segurança de hardware (HSMs)" refere-se a dispositivos criptográficos seguros usados em processamento de PIN, personalização de cartões, gestão de chaves criptográficas e proteção de dados.
- "Dispositivos de segurança de pagamento" refere-se coletivamente a dispositivos de POI e HSMs.
- "Segurança em Transações com PIN" refere-se à estrutura dentro dos padrões da PCI e aos requisitos que lidam com a avaliação e a aprovação de dispositivos de segurança de pagamentos.

1.4 Sobre o PCI Security Standards Council

O Conselho de Padrões de Segurança da Indústria de cartões de pagamento (PCI) estabeleceu a estrutura de segurança em transações com PIN, para lidar com a avaliação de segurança e aprovação de dispositivos de segurança de pagamentos.

Este *Guia do Programa de teste e aprovação de dispositivos de segurança em transações com PIN da Indústria de cartões de pagamento* reflete um alinhamento com as marcas de pagamento participantes em um conjunto padrão de:

- Requisitos de segurança,
- Metodologias de teste e
- Processos de aprovação

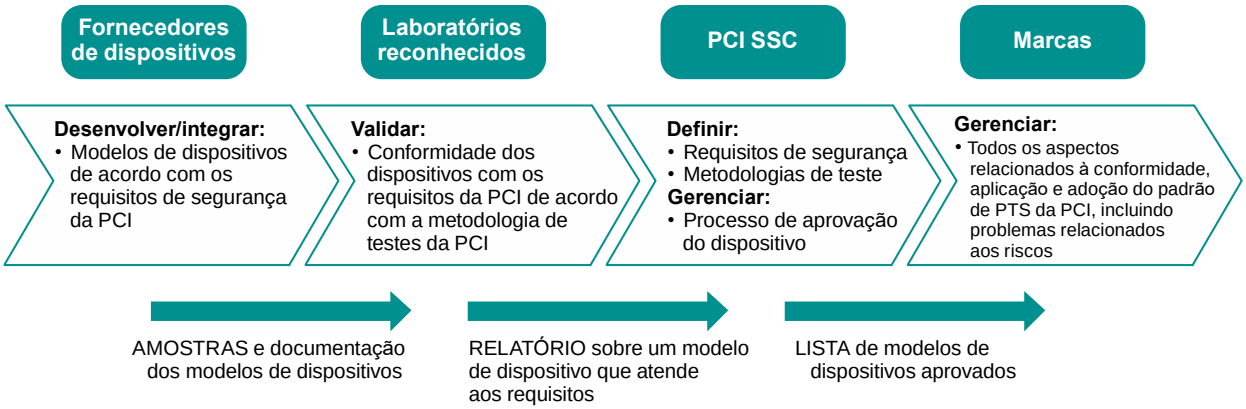
Observação:
As aprovações são concedidas diretamente por meio do PCI SSC e são coordenadas pelas marcas de pagamento participantes da PCI através do processo do programa de PTS da PCI.

Todos os dispositivos enviados para avaliações de segurança e aprovação foram avaliados de acordo com os Requisitos de Segurança de PTS da Indústria de cartões de pagamento (PCI) alinhados e aplicáveis. As Listas de Aprovação da PCI disponibilizam uma lista completa de dispositivos de segurança de pagamento reconhecidos como em conformidade com os Requisitos de PTS da PCI.

Esse esforço colaborativo assegura que todos os dispositivos de segurança de pagamento sejam avaliados sob um processo em comum que oferece um alto grau de garantia. O objetivo do acordo a melhoria da segurança global para o titulares de cartões e outros dados confidenciais, eliminando requisitos conflitantes. Todos os participantes da cadeia de valor de pagamentos se beneficiam dos requisitos alinhados:

- Os clientes são beneficiados por uma seleção mais ampla de dispositivos seguros.
- Os comerciantes, as instituições financeiras, os processadores e demais terceiros têm a certeza de que usarão produtos que atenderam ao nível de garantia exigido.
- Os fornecedores podem reduzir o “tempo de comercialização” de novos dispositivos, pois deverão concluir somente uma única avaliação de segurança e um único processo de aprovação.

1.5 Regras de marcas de pagamento

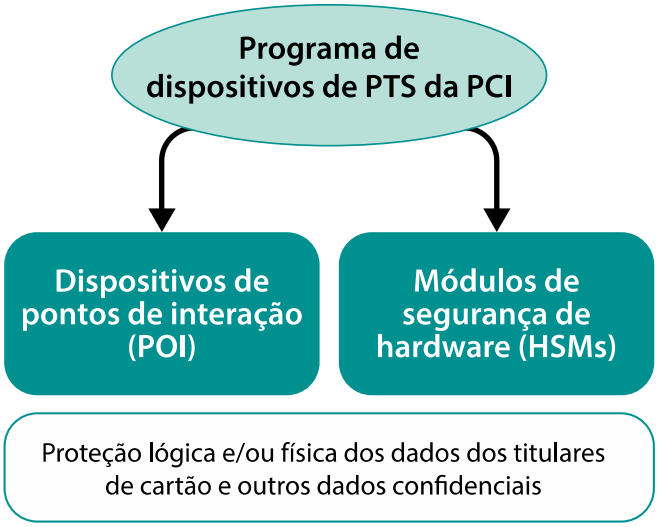


Todos os aspectos que se relacionam com o cumprimento, a aplicação e a adoção dessas normas, inclusive todas as questões relacionadas com riscos, são de responsabilidade das marcas individuais de cartões de pagamento. A imagem a seguir apresenta uma descrição de alto nível da cadeia de segurança do dispositivo.

2 Descrição do processo de teste e aprovação

2.1 Visão geral

A estrutura de aprovação de segurança de PTS do PCI SCC lida com a proteção lógica e/ou física de titulares do cartões e outros dados sensíveis nos dispositivos de ponto de interação (POI) e módulos de segurança de hardware (HSMs), como indicado no diagrama abaixo.



Exceto onde indicado, este documento refere-se a dispositivos de POI e HSMs como “dispositivos de segurança de pagamento”.

Os fornecedores de dispositivos que desejarem ter seus modelos de dispositivo aprovados pelo PCI SSC podem entrar em contato com um dos laboratórios reconhecidos pela PCI e preencher os formulários apropriados da PCI (incluídos nos *Requisitos de Segurança PCI PTS*). O fornecedor enviará então o dispositivo, junto com toda a documentação adicional exigida pelo laboratório, para avaliação e validação da conformidade com os Requisitos de Segurança PCI PTS. Após a conclusão da avaliação, o PCI SSC revisará o relatório da avaliação. Se o modelo do dispositivo atender aos requisitos da PCI, será aprovado e listado no site da PCI PTS. Uma carta de aprovação será emitida confirmando a conclusão bem-sucedida do processo.

2.2 Antes do teste (somente dispositivos de POI)

- O PCI SSC recomenda que o dispositivo de POI receba antes a aprovação EMV de Nível 1, se aplicável, e depois a aprovação da PCI, antes de enviá-la para qualquer teste EMV de Nível 2 apropriado. (No que diz respeito à aprovação EMV de Nível 1, deve haver pouca ou nenhuma sobreposição nos processos de teste com a aprovação de segurança PCI PTS POI.)
- Se o dispositivo de POI puder trabalhar com ambos os tipos de opções de entrada de PIN, online e offline, informe ao laboratório para que avalie ambos ao mesmo tempo, ou que o laboratório indique compatibilidade futura para ambas as opções no relatório de avaliação. Para que a aprovação do dispositivo de POI possa indicar a compatibilidade de ambas as opções, o fornecedor deverá garantir que, após a segunda avaliação da opção de entrada de PIN ser realizada, o laboratório deverá incluir ambos em seu relatório.

2.3 A abordagem modular

A abordagem modular do de PTS da PCI apresenta um processo abrangente de avaliação para abordar a diversidade de arquiteturas dos dispositivos de segurança de pagamento, das opções de produtos e dos modelos de integração. Possivelmente, otimiza os custos de avaliação e o tempo que os laboratórios passam revisando arquiteturas não convencionais, a aprovação pela PCI de tipos de produto e a manutenção das aprovações atuais (alterações nos componentes de segurança, etc).

A abordagem modular de PTS da PCI é compatível com a apresentação de dispositivos em conformidade com os tipos de produtos e as classes de homologação definidos no Apêndice A.

Tabela 1: módulos de avaliação

Para poder capturar a diversidade de requisitos de segurança em um único processo de avaliação de conformidade pelo laboratório, os Requisitos de Segurança de PTS POI dividem-se nos seguintes módulos de avaliação:

Requisitos e nome do módulo de avaliação	Descrição
Segurança física	Requisitos da segurança física dos dispositivos de POI
Segurança Lógica	Requisitos da segurança lógica dos dispositivos de POI
Requisitos de integração do dispositivo	Asseguram que a integração dos componentes previamente aprovados não prejudique a segurança geral, conforme indicado nos requisitos de segurança, e inclui os requisitos de gerenciamento de segurança aplicáveis ao dispositivo integrado.
Comunicações e interfaces	A interface dos terminais de POI para abrir redes com protocolos abertos
Ciclo de Vida	Leva em consideração como o dispositivo é produzido, controlado, transportado, armazenado e utilizado durante todo o seu ciclo de vida.

Qualquer um dos produtos que incorporar módulos separados, como um EPP, leitores de cartões, etc., deverá atender aos requisitos de integração.

Os produtos compatíveis com protocolos abertos ou que procuram obter a designação segura de leitura e intercâmbio de dados (SRED) devem ser avaliados de acordo com os requisitos de segurança relevantes, conforme designado no Apêndice B: Aplicabilidade dos Requisitos nos *Requisitos de Segurança Modular de POI de PTS*. Consulte as colunas “Implementa Protocolos Abertos” e “Protege os dados da conta” para ver os requisitos que devem ser atendidos, além de outros requisitos envolvidos.

Qualquer método de comunicação que faça uso de uma rede sem fio, local ou de área ampla para transportar dados está sujeito à avaliação de protocolos abertos. Isso inclui, entre outros, Bluetooth, Wi-Fi, rede celular (GPRS, CDMA) ou Ethernet. Uma conexão serial ponto a ponto dispensaria avaliação, a menos que essa conexão fosse sem fio ou por meio de um hub, switch ou outro dispositivo multiporta. Além disso, toda comunicação que utilizar um protocolo de domínio público ou um protocolo de segurança também seria avaliada com os requisitos vigentes dos protocolos abertos.

Há vários cenários em que o SRED é obrigatório. Tais cenários incluem todos os dispositivos validados para as classes de aprovação não ligados a PED ou SCR, ou em alguns cenários portáteis que envolvem um dispositivo de entrada de PIN conectado (como por meio de encaixes deslizantes, invólucros ou conectores de áudio) a um telefone celular, PDA ou terminal de PDV.

O objetivo geral do requisito de validação SRED é garantir que as implementações de proteção de dados de contas sejam totalmente robustas, como evidenciado pela validação e aprovação de acordo com os requisitos da SRED. No entanto, o objetivo do requisito não é inibir o fornecedor de implementar proteções de dados de conta insuficientes para atender aos requisitos da SRED vigentes, mas que ainda podem fornecer um nível menor de proteção para os dados da conta. Assim, um fornecedor que implementa proteções de dados da conta e ***não*** busca a SRED como uma função aprovada fornecida, poderá fazê-lo.

2.4 Procedimentos de teste

Os dispositivos de segurança de pagamento são avaliados pelo uso dos requisitos incorporados nos *Requisitos de segurança modular de POI de PTS da PCI* ou o manual *Requisitos de segurança do módulo de segurança de hardware da PCI* ("manual HSM"), conforme aplicável. O laboratório verificará as respostas "SIM" ou "N/A" do fornecedor nessas seções, fazendo com que o fornecedor apresente evidências adicionais de conformidade com os requisitos, conforme indicado por meio das informações e das amostras de dispositivos de segurança de pagamento necessárias. Nenhum relatório será aceito com "Não" como resposta.

Qualquer um dos produtos que incorporar módulos separados, como EPPs, leitores de cartões, etc., deverá atender aos requisitos de integração. Os produtos não precisam ser compatíveis com protocolos abertos ou com leitura e intercâmbio de dados seguros; no entanto, se forem, esses requisitos serão obrigatórios para avaliação e aprovação.

Os fabricantes de terminais podem fazer a compra de componentes seguros aprovados pela PCI de vários fornecedores e integrá-los a suas soluções finais, e eles próprios podem ser aprovados de acordo com os requisitos PCI PTS.

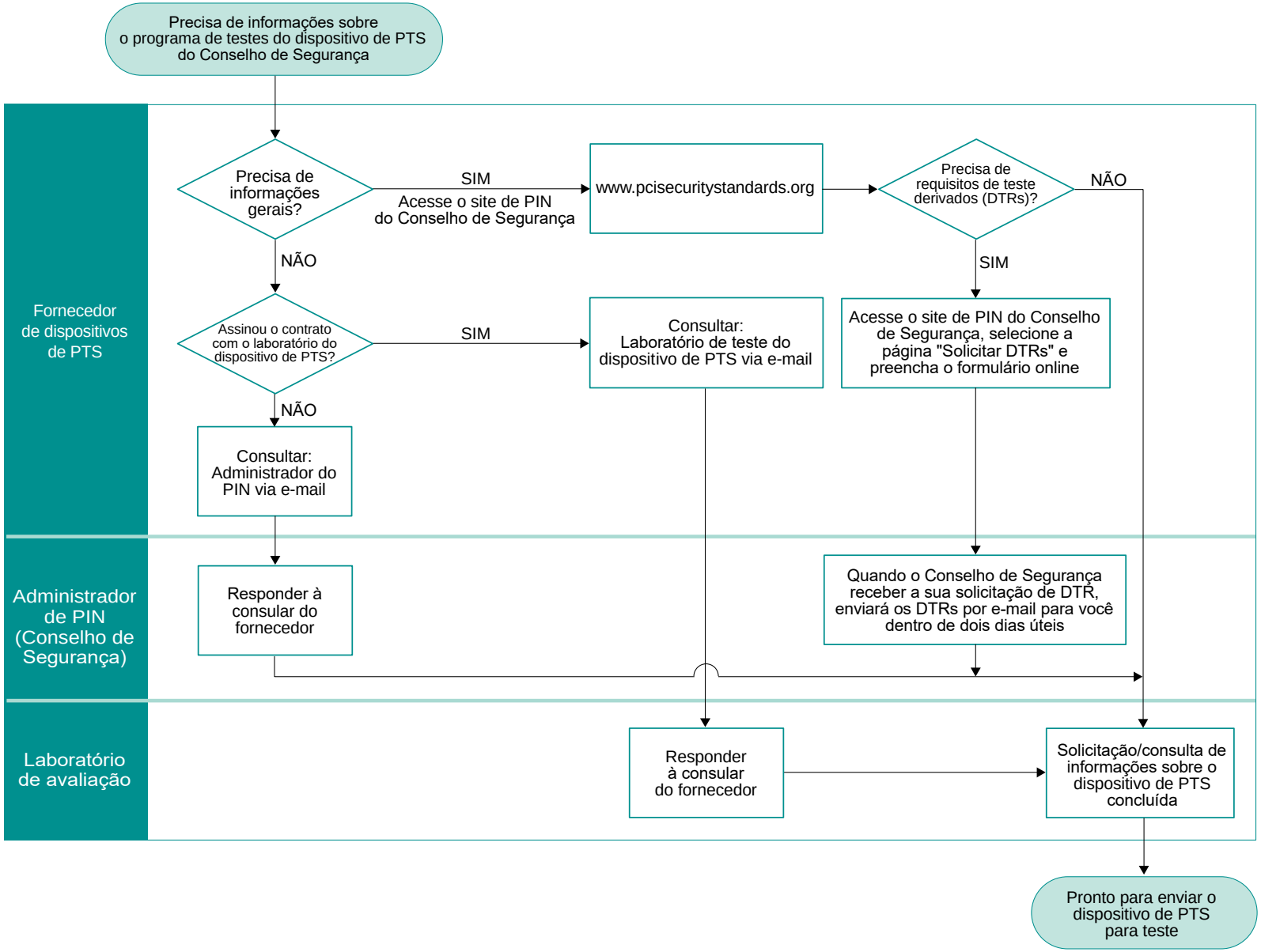
O laboratório validará os dispositivos de segurança de pagamento de acordo com os Requisitos de ciclo de vida, conforme especificado nos *Requisitos de segurança modular de POI de PTS da PCI*ou *Requisitos de Segurança PCI HSM.* Isso é feito por meio de revisões de documentação e por meio de evidências de que os procedimentos são devidamente implementados e utilizados. Quaisquer variações a esses requisitos serão relatadas à PCI para revisão. Essas informações são necessárias como parte do processo de aprovação.

Tabela 2: ilustração do processo de teste e aprovação

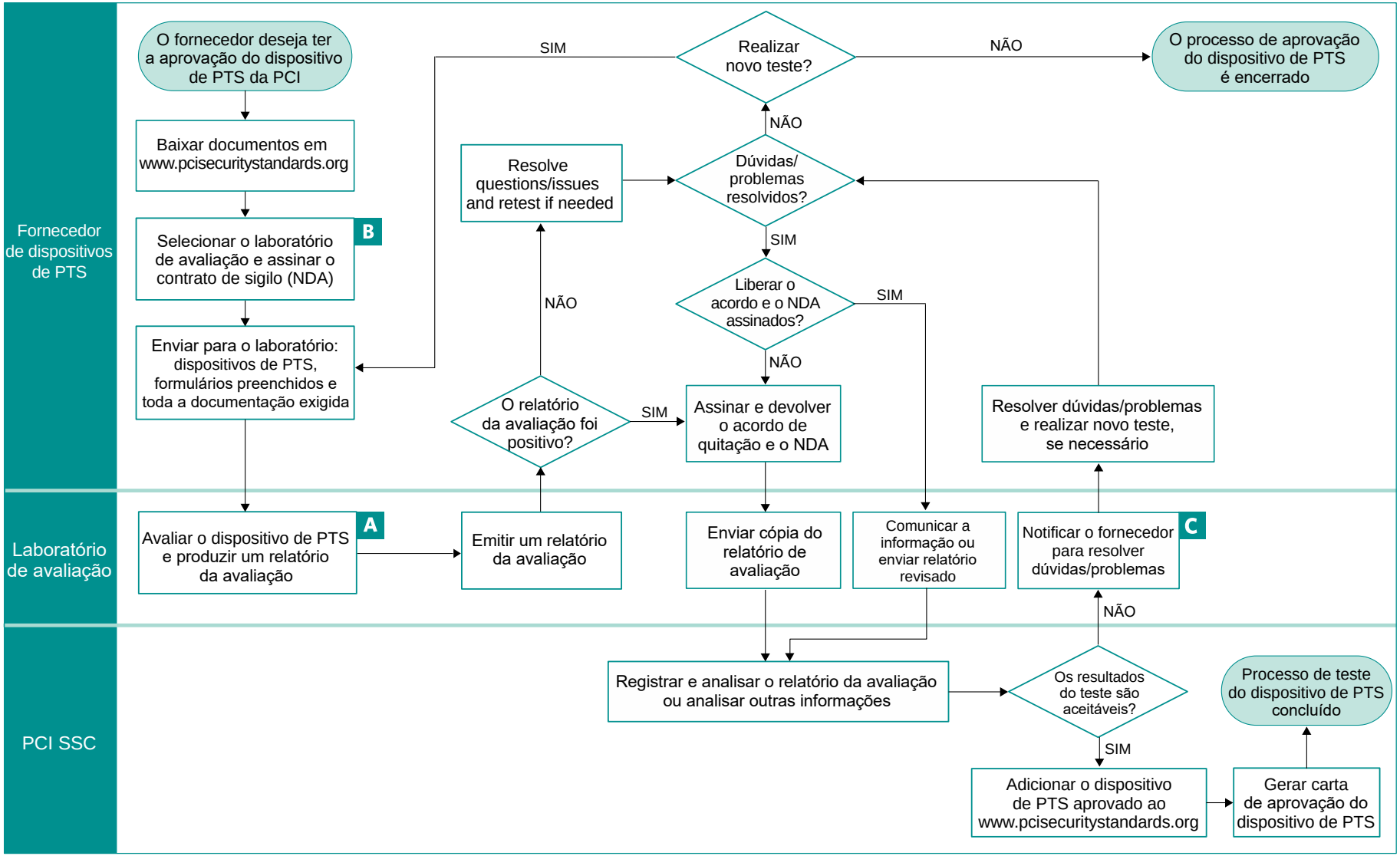
A tabela abaixo e os gráficos nas páginas que se seguem descrevem e ilustram o processo de teste e aprovação do dispositivo de segurança de pagamento.

Estágio do Processo	Recursos/Explicação	Ilustração
Antes do teste	Descrição do processo de teste e aprovação	Figura 1
Obter documentação e formulários apropriados	Processo detalhado de avaliação	Figura 2
Entre em contato com um laboratório de testes reconhecido pela PCI para começar o teste	Preparação para testes	Figura 2
Assinar NDA e acordo de liberação	Processo de aprovação	Figura 2
Enviar documentação e materiais	Requisitos para testes	Figura 2
Responder a consultas do laboratório de testes	Suporte técnico durante o teste todo	Figura 2
Receber resposta ou carta de aprovação do PCI SSC	Processo de Aprovação	Figura 2
Alterações em dispositivo PTS	Alterações a um dispositivo PTS previamente aprovado	Figura 3

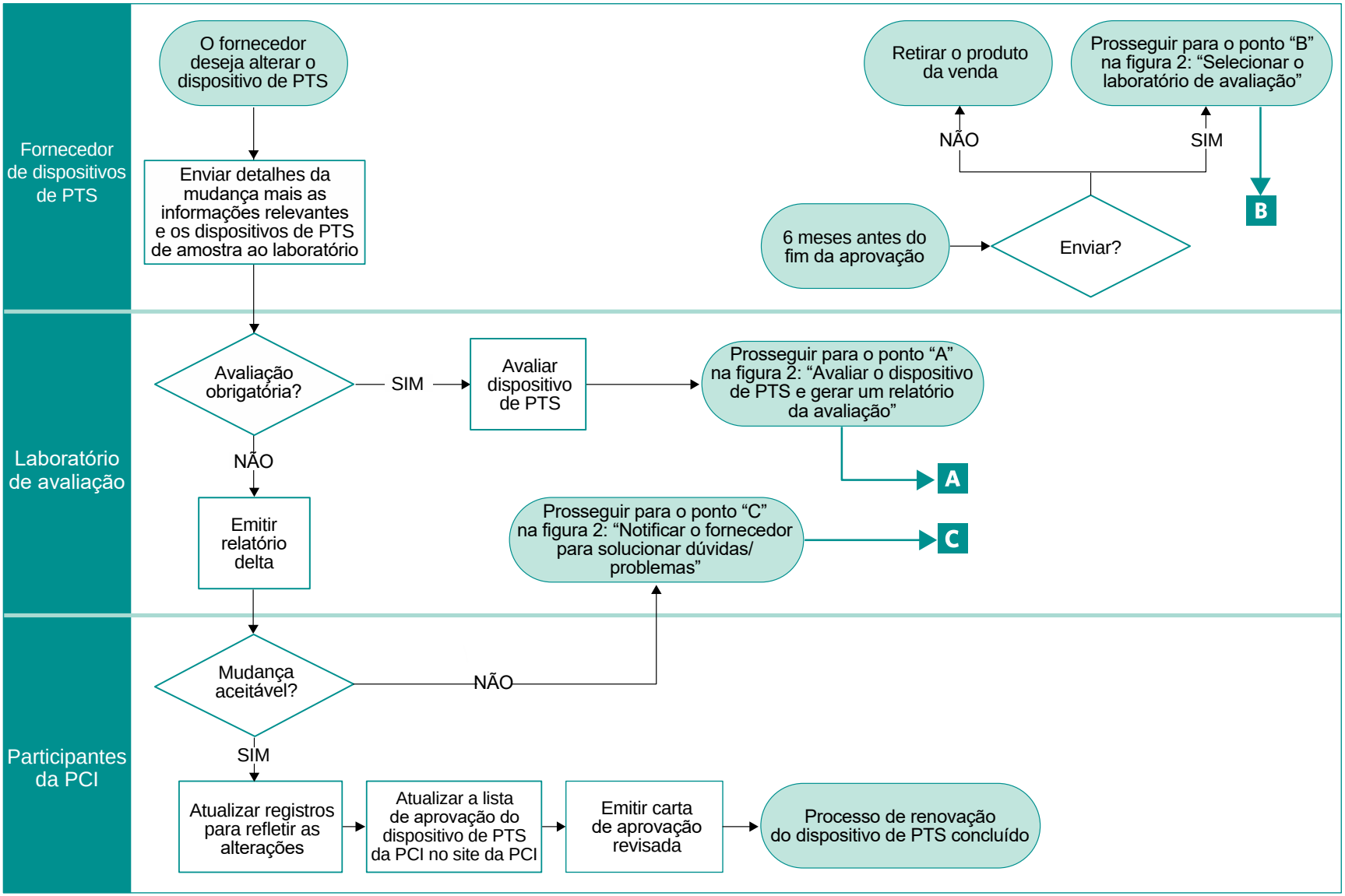
2.5 Figura 1: fluxograma da consulta do teste de dispositivo PTS



2.6 Figura 2: fluxograma de aprovação de dispositivo PTS



2.7 Figura 3: Fluxograma de solicitação e renovação de alteração do dispositivo de PTS



3 Processo de avaliação detalhada

Os dispositivos de segurança de pagamento serão avaliados de acordo com os *Requisitos de segurança modular de POI de PTS da PCI*ou o manual *Requisitos de segurança do módulo de segurança de hardware da Indústria de cartões de pagamento* . O laboratório avaliará as respostas do fornecedor nessas seções, fazendo com que o fornecedor apresente evidências adicionais de conformidade com os requisitos por meio de informações e das amostras de dispositivos de segurança de pagamento necessárias. O PCI SSC analisará o relatório de avaliação do dispositivo de segurança de pagamento apropriado do laboratório. Se os resultados forem satisfatórios, o dispositivo de segurança de pagamento será aprovado e o dispositivo PTS será publicado como um dispositivo de segurança de pagamento “aprovado pela PCI” em www.pcisecuritystandards.org . Uma carta de aprovação será então emitida ao fornecedor.

As Dúvidas técnicas frequentes são uma parte integrante do processo de avaliação. As Dúvidas técnicas frequentes são identificadas pela versão principal dos requisitos de segurança, como 4.x, 5.x, 6.x. Cada versão das Dúvidas técnicas frequentes é específica da versão principal correspondente aos requisitos de segurança. Por exemplo, As Dúvidas técnicas frequentes da versão 6 são específicas dos requisitos de segurança da versão 6.x e somente dos requisitos de segurança da versão 6.x, e assim por diante.

As Dúvidas técnicas frequentes são atualizadas periodicamente e entram geralmente em efeito após a publicação. Dependendo da natureza da Dúvida Frequente (como esclarecimento versus abordar uma ameaça eminente), sua aplicabilidade pode ser deslocada para dispositivos em avaliação no momento da publicação.

Modificações para dispositivos aprovados, chamados de “deltas”, podem ocorrer a qualquer momento durante a aprovação do produto. Os dispositivos que passam por avaliações delta devem levar em conta as dúvidas frequentes atuais da versão principal associada dos requisitos de segurança somente para os requisitos de segurança que forem afetados pela alteração delta. Por exemplo, se uma alteração afetar a conformidade com os requisitos B1 e B4, apenas as dúvidas frequentes atuais associadas a B1 e B4 deverão ser consideradas como parte do delta.

Os dispositivos para os quais a homologação tiver expirado também poderão passar por deltas. Isso acontece porque os fornecedores podem precisar fazer correções de manutenção em dispositivos que o fornecedor já vendeu, mas ainda devem fornecer suporte para. Em adição, os fornecedores podem optar por portar versões atualizadas do firmware que foram aprovadas em relação aos requisitos de segurança mais recentes para produtos para os quais a aprovação expirou. Isso pode acontecer porque os clientes de um fornecedor desejam padronizar sua implantação em relação a uma determinada versão do firmware e/ou adicionar funcionalidade a esse dispositivo.

Depois da publicação de uma nova versão importante (por exemplo, 4.x, 5.x, 6.x), haverá um período de doze meses de sobreposição com a versão existente, começando no mês do ano em que a versão principal mais recente for publicada. Os fornecedores podem optar durante esse período por enviar um dispositivo sob qualquer versão dos requisitos de segurança. A exceção para isso são os SCRPs, que para novas aprovações devem sempre utilizar a versão mais atual dos Requisitos de Segurança. Doze meses depois da publicação da nova versão principal, a versão mais antiga dos requisitos de segurança estará disponível somente para avaliações delta.

No ano em que os requisitos anteriores forem retirados de uso, qualquer fornecedor que estiver utilizando esses requisitos para uma nova avaliação deverá ter o dispositivo em avaliação sessenta dias antes da data de retirada da versão, e a PCI deverá ser notificada por escrito por cada laboratório reconhecido pela PCI dos dispositivos específicos que eles têm sob avaliação. Os relatórios finais de avaliação de laboratório devem ser recebidos pela PCI até ao final desse cronograma de sessenta dias. Se os dispositivos precisarem de mudanças com base na revisão PCI dos relatórios de avaliação, essas mudanças poderão ser feitas após esse cronograma de sessenta dias. No entanto, a PCI não deve aceitar nenhum relatório de avaliação revisado após sessenta dias após a retirada da versão principal anterior.

A partir de 31 de janeiro, o fornecedor deve preencher e enviar à PCI um Atestado de Validação (AOV — ver Apêndice D) confirmando a adesão ao guia do programa — ou seja, o firmware não foi alterado ou as alterações feitas estão dentro dos parâmetros curinga ou foram submetidas para avaliação. O processo de vulnerabilidade, relatado no AOV, deve incluir todas as interfaces físicas e seus protocolos lógicos correspondentes conforme definido em D1. Para dispositivos que dão suporte a protocolos abertos, o fornecedor deve apresentar materiais de evidência de que existe um registro auditável de um processo de avaliação de vulnerabilidade contínuo fornecendo uma cópia do formulário de aprovação do fornecedor especificado no Requisito E10. Isso se aplica a todas as aprovações existentes que não expiraram para o fornecedor a partir de 31 de dezembro do ano anterior. O não envio do AOV anual significa que os envios de relatórios adicionais do fornecedor não serão processados. Não é necessário um AOV para dispositivos que estão no fim da vida útil, conforme enumerado na Seção 5.

Em vigor com o POI v6, o firmware expira em 31 de dezembro a cada terceiro ano subsequente ao ano inicialmente aprovado. Por exemplo, as versões de firmware aprovadas durante 2020 expirarão em 31 de dezembro de 2022, 31 de dezembro de 2025 e 31 de dezembro de 2028. Essa expiração independe da data de validade geral do dispositivo — consulte a Seção A.12. Para que não expire, o firmware deve ser avaliado em laboratório com base nas seguintes DTRs e o relatório enviado e aprovado pela PCI antes de 1 de maio do ano seguinte à expiração:

Observação:

Esta avaliação complementa o AOV anual.

DTR B16	Separação do aplicativo
DTR B17	Configuração mínima
DTR B22	Acesso remoto
DTR D2	Anomalias lógicas
DTR E10	Procedimentos de avaliação da vulnerabilidade do fornecedor
DTR E11	Avaliação da vulnerabilidade de todas as interfaces
DTR E12	Divulgação de vulnerabilidade

Além disso, os fornecedores podem ser solicitados pelas entidades que compram seus dispositivos a concluir um atestado de dispositivos PTS — ver Apêndice E. Esse documento é para que os fornecedores atestem que as versões de hardware e firmware dos dispositivos que estão sendo comprados estão de acordo com os números de versão listados no site do PCI para esse nome/número de modelo de dispositivo específico

3.1 Documentação e materiais obrigatórios

Todas as informações e documentos relevantes para o Programa de Teste e Aprovação PCI PTS podem ser baixados de www.pcisecuritystandards.org . Todos os formulários e questionários preenchidos relacionados à avaliação do dispositivo de segurança de pagamento devem ser entregues a um laboratório de testes reconhecido pela PCI e não ao PCI SSC. As informações específicas da avaliação devem ser solicitadas diretamente ao laboratório reconhecido pela PCI.

Exemplos de documentos e itens a serem enviados a um laboratório de teste de dispositivo de segurança de pagamento reconhecido pela PCI incluem, conforme aplicável, para a classe de aprovação do dispositivo:

1. Formulários apropriados preenchidos *de Requisitos de Segurança PCI* para o dispositivo.
2. Questionário de Fornecedor de laboratório preenchido para o dispositivo.
3. Uma política de segurança disponível pelo usuário para publicação com a aprovação em www.pcisecuritystandards.org . O documento deve conter no mínimo todas as informações prescritas nos Requisitos de Teste Derivados aplicáveis.
4. Três (3) dispositivos de POI de trabalho (para HSMs, consulte o laboratório) com o manual ou as instruções do operador. Além disso, para dispositivos de POI enviados a novas avaliações, o fornecedor deve fornecer dois dispositivos de trabalho para o laboratório para arquivamento pela PCI conforme descrito abaixo.
5. Os acessórios necessários de hardware e software para realizar transações de pagamento baseadas em PIN simuladas (para HSMs, consulte o laboratório).
6. A documentação que descreve todas as funções utilizadas para entrada e saída de dados que podem ser usadas por desenvolvedores de aplicativos de terceiros. Especificamente, funções associadas à gestão de chaves, gestão de PIN e interfaces de usuário (como tela e teclado) devem ser descritas. (Um manual de API é um exemplo da documentação que pode preencher esse requisito.)
7. A documentação relacionada ao “processo, que pode ser auditado”. Exemplos dessa documentação incluem:
    - Procedimentos de qualidade de software
    - Procedimentos de controle de documentação e software
    - Formulários de alteração
    - Registros controle de mudanças
    - Registros de mudanças
8. As instruções e os acessórios (como carregadores de chaves) que permitirão que os engenheiros do laboratório de teste usem todos os modos especiais que o dispositivo de segurança de pagamento suporta, incluindo carregamento de chaves, seleção de chaves, zeroização de chaves e outras funções de gerenciamento e manutenção de chaves.
9. Documentação adicional, como por exemplo (a) diagramas de blocos, esquemas e fluxogramas, que ajudarão na avaliação do dispositivo de segurança de pagamento e (b) fator de forma do dispositivo e imagens relacionadas para a publicação (se aprovada pelo PCI SSC) na Lista de Aprovação de Dispositivos PTS e uso relacionado do PCI SSC. O laboratório pode solicitar material adicional de avaliação quando necessário.

Aplicável somente a dispositivos de POI:

Depois de uma avaliação bem sucedida, o laboratório de testes da PTS deve fornecer ao Conselho dois dispositivos de amostragem. O endereço para envio e o contato local estão indicados abaixo. Os dados experimentais de certos testes realizados devem ser conservados para futuras disposições ao Conselho, conforme o necessário. Isto se aplica a todas as novas avaliações que resultam em um número novo de aprovação. Não se aplica a deltas. Não se aplica tampouco a uma situação em que o fornecedor estiver fazendo tão somente o rebranding do produto previamente aprovado de outro fornecedor. Contudo, se um fornecedor estiver fazendo rebranding de um produto e, além disso, fizer outras alterações, como no firmware, se aplicará. Detalhes e atualizações adicionais sobre essas questões estarão disponíveis nas comunicações da PCI para Laboratórios e Fornecedores. São resumidos da seguinte forma:

- **Amostras de dispositivos:** dois (2) terminais contendo as mesmas chaves e aplicativos que os fornecidos ao laboratório reconhecido pela PCI. Isso inclui todas as classes de aprovação. Para itens grandes, notifique por meio dos detalhes de contato abaixo antes do envio. Se um dispositivo tiver variantes diferentes, o laboratório deverá enviar duas variantes diferentes, selecionando as duas que mais representam o intervalo de todas as variantes. O fornecimento de amostras de dispositivos é uma parte necessária da aprovação de um dispositivo. Estes serão mantidos de forma segura e podem ser usados para avaliar a vulnerabilidade a novas técnicas de ataque. Se um modelo for comprometido no campo, as amostras retidas podem ser usadas para investigar qualquer comprometimento ou violação de segurança.
- O**Teste robusto do canal lateral** é uma parte importante da avaliação do dispositivo. Os dados de teste de canais laterais relevantes (formas de onda representadas digitalmente e dados numéricos associados) produzidos por uma avaliação devem ser armazenados pelo laboratório durante, pelo menos, seis meses após a aprovação do dispositivo. O Conselho solicitará que alguns ou todos esses dados sejam fornecidos, se necessário. Os laboratórios devem comunicar com o Conselho a fim de resolver quaisquer questões sobre este assunto.
- **O teste robusto de anomalias lógicas** é uma parte importante da avaliação do dispositivo. Exemplos relevantes de dados de fuzzing (dados de saída e/ou registros, relatórios, etc.), fornecendo um resumo representativo e compreensível das execuções de teste de ataque fuzzing devem ser apresentados nos relatórios de avaliação que o acompanham, indicando quais testes foram realizados e por quê, e com detalhes suficientes para explicar os testes fundamentação e conclusões.

Enviar os dispositivos para:	Informações de contato para envio:
Attn: MasterCard Global Products and Solutions MasterCard Worldwide 5 Booths Park Chelford Road Knutsford Cheshire WA16 8QZ Reino Unido	Contato: Sra. Deborah Corness Telefone: +44 (0)1565 626500 Fax: +44 (0)7738 202 663 E-mail: deborah_corness@mastercard.com

4 Preparação para Testes

4.1 Serviços de laboratório

Para facilitar o processo de avaliação antes dos testes reais, um laboratório reconhecido pela PCI pode oferecer os seguintes serviços:

- Orientação sobre o projeto de dispositivos de segurança de pagamento para estar em conformidade com os requisitos de segurança da PCI
- Revisão do design do dispositivo de segurança de pagamento de um fornecedor, resposta a perguntas por e-mail ou telefone e participação em chamadas em conferência para esclarecer os requisitos
- Uma avaliação preliminar de segurança física no equipamento de um fornecedor
- Direcionamento sobre como colocar os dispositivos de segurança de pagamento de um fornecedor em conformidade com os requisitos da PCI se as áreas de não conformidade forem identificadas durante a avaliação.

Os fornecedores são motivados a entrar em contato diretamente com um laboratório reconhecido pela PCI em relação aos serviços acima e quaisquer taxas associadas a eles. No entanto, os laboratórios **não podem** oferecer nenhum conselho sobre o design real do dispositivo de POI ou HSM.

4.2 Laboratórios reconhecidos pela PCI

APCI SSC reconhece atualmente uma série de laboratórios para testes de dispositivos PTS. A lista atual de laboratórios de teste PTS reconhecidos encontra-se no site do PCI SCC, na seção "Dispositivos aprovados pela PTS".

4.3 Taxas de teste

Todas as taxas e datas referentes ao teste são negociadas entre o fornecedor e o laboratório e o fornecedor paga todas as taxas diretamente ao laboratório. Se uma discrepância exigir que o fornecedor modifique o design físico do dispositivo de segurança de pagamento ou o firmware, o dispositivo de segurança de pagamento deverá ser reenviado para um novo ciclo de testes e o laboratório faturará o fornecedor em conformidade.

Observação:

O fornecedor paga todas as taxas de avaliação de laboratório diretamente ao laboratório.

4.4 Requisitos para Testes

Como requisito para testes, o fornecedor do dispositivo de segurança de pagamento deve fornecer a documentação e as amostras apropriadas para o laboratório. Consulte "Documentação e Materiais Obrigatórios" para mais informações.

O laboratório de testes pode desempenhar uma pré-avaliação de um dispositivo de segurança de pagamento de fornecedor e decidir que há deficiências que impediriam uma aprovação. O laboratório pode então dar a resposta ao fornecedor com uma lista de todos os aspectos do dispositivo de segurança de pagamento que devem ser abordados antes do início do processo formal de teste.

4.5 Datas de teste

Os fornecedores que enviaram dispositivos para testes em um laboratório reconhecido pela PCI receberão uma data de teste do laboratório. Os fornecedores devem notificar diretamente o laboratório sobre qualquer atraso na apresentação de dispositivos de segurança de pagamento para testes.

4.6 Prazos de teste

Uma nova avaliação pode geralmente começar dentro de duas semanas após a recepção de todos os itens do laboratório para testes. Os intervalos de tempo devem ser agendados com o laboratório com antecedência. O tempo real de avaliação variará de acordo com o escopo da avaliação e a rapidez do fornecedor. As avaliações podem ser realizadas de forma mais rápida se o laboratório tiver toda a documentação e o hardware necessários, e se não houver problemas significativos de conformidade.

Os prazos para teste são estimativas baseadas na suposição de que o dispositivo de segurança de pagamento conclui com êxito os testes. Se forem encontrados problemas durante o teste, poderá ser necessário haver discussões entre o laboratório e o fornecedor. Essas discussões podem afetar os tempos de teste e causar atrasos e/ou encerrar o ciclo de ensaio antes da conclusão de todos os testes.

4.7 Definições do ciclo de testes

Todos os dispositivos de segurança de pagamento são necessários para completar um ciclo de testes com resultados bem-sucedidos como parte do Programa de teste e aprovação da PCI. **Um ciclo de testes** é definido como a conclusão de todos os procedimentos de teste aplicáveis executados em uma única versão do dispositivo de segurança de pagamento do fornecedor. Quando um único ciclo de testes é concluído sem quaisquer discrepâncias descobertas, o fornecedor é avisado que o dispositivo de segurança de pagamento concluiu com êxito um ciclo de testes.

Durante o processo de teste, todos os procedimentos de teste aplicáveis são desempenhados de acordo com os*Requisitos de teste derivados aplicáveis da PCI*. Todas as discrepâncias descobertas são relatadas ao fornecedor. Todos os ensaios aplicáveis devem ser realizados durante um único ciclo de ensaio, a menos que:

- Um erro de aplicativo faça com que todos os testes dentro de uma parte do código lógico do software funcionem incorretamente, impedindo testes adicionais dentro dessa área do aplicativo.
- O dispositivo de segurança de pagamento apresente uma falha catastrófica que impeça qualquer continuação dos testes.
- O teste exceda o comprimento do ciclo de testes programado.
- O fornecedor solicita o fim do ciclo de testes.

Se um ciclo de testes tiver terminado com descoberta de discrepâncias, o fornecedor será notificado de que o dispositivo de segurança de pagamento falhou no ciclo de testes. O laboratório emitirá um relatório final que trata as discrepâncias.

Não há nenhuma disposição para interromper o ciclo de testes e reiniciar o ciclo novamente em uma data posterior.

4.8 Suporte Técnico durante o Teste Todo

O laboratório, a seu critério, pode procurar informações adicionais do fornecedor que possam resolver a discrepância. Se a discrepância exigir que o fornecedor modifique o projeto físico do dispositivo de segurança de pagamento ou o firmware, o dispositivo de segurança de pagamento deverá ser reenviado para um novo ciclo de testes e o laboratório faturará o fornecedor de forma correspondente.

Recomenda-se que o fornecedor disponibilize uma pessoa de recursos técnicos para ajudar com quaisquer perguntas que possam surgir durante os testes laboratoriais. Durante a avaliação e para agilizar o processo, o contato do fornecedor deve estar “de plantão” para discutir discrepâncias e responder as dúvidas do laboratório.

Os trabalhos de avaliação de laboratório devem ocorrer utilizando pessoal e equipamento de laboratório aprovados. Os testes de dispositivos para aprovações PTS devem ser efetuados na instalação de laboratório reconhecida pela PCI e não no local do fornecedor, a menos que:

- O trabalho do laboratório está relacionado à avaliação das políticas e dos procedimentos do fornecedor.
- Avaliação dos requisitos de segurança de ciclo de vida.
- Quando necessário, rever o código-fonte.

Todos os trabalhos concluídos fora da instalação do laboratório reconhecido pela PCI devem estar claramente documentados no relatório de avaliação do dispositivo de PTS da PCI.

5 Taxas PCI

Os fornecedores recebem uma cobrança de taxa para cada novo relatório de avaliação recebido. Além disso, os fornecedores recebem uma cobrança de taxa anual de listagem ou manutenção para cada aprovação PCI existente. Estas taxas são estipuladas em www.pcisecuritystandards.org/fees.

5.1 Delitos

Os fornecedores que estiverem devendo pagamentos ao PCI SSC não deverão ter nenhum relatório processado pela PCI até que façam os pagamentos. Além disso, o PCI SSC pode cobrar penalidades, taxas e juros para fornecedores em atraso.

5.2 Novas avaliações

A taxa para novas avaliações será uma taxa de passagem pelo laboratório de testes aplicável para o fornecedor. O laboratório de testes fornecerá os valores ao PCI SSC e cobrará essas taxas como parte da taxa de avaliação. A taxa será cobrada a cada três meses para todas as novas avaliações enviadas pelo laboratório nos três meses anteriores. Os fornecedores não deverão pagar por modificações de hardware ou firmware nas aprovações existentes da PCI, denominadas aprovações “delta”.

5.3 Avaliações iniciais em versões principais

Todas as avaliações iniciais sob uma versão principal (por exemplo, 5.x, 6.x, etc.) dos requisitos de segurança para um certo produto devem constituir uma nova avaliação e devem receber um novo número de aprovação e ser faturadas em conformidade. As avaliações delta não podem levar um produto previamente aprovado sob um número de versão principal anterior, por exemplo, 5.x, para uma aprovação sob outro número de versão principal, por exemplo, 6.x.

5.4 Taxa de aprovação de listagem

A taxa de listagem de aprovação será cobrada a cada seis meses pelo PCI SSC. As datas de cobrança serão fixadas como 1.º de maio e 1.º de novembro de cada ano. Os fornecedores pagarão o valor total de todas as aprovações da PCI não expiradas existentes em 30 de abril para cobrir o período de 1.º de maio até 30 de abril. O faturamento de 1.º de novembro cobrirá todas as novas listagens que forem publicadas de 1.º de maio a 31 de outubro. Os fornecedores com novas listagens publicadas durante esse período receberão uma fatura pro-rata com base na data de efetivação do anúncio.

Todos os dispositivos aprovados para os quais a aprovação não tiver expirado deverão ter uma taxa de cobrança de aprovação para todas as aprovações existentes a partir de 1.º de maio. Os fornecedores não pagarão a taxa de listagem anual para produtos em “Fim da Vida Útil” (EOL) sobre os quais tiverem notificado a PCI por escrito noventa (90) dias antes da data de faturamento de 1.º de maio. Um produto em fim da vida útil é um produto que não é mais comercializado para novas implantações, conforme descrito na Seção A.13 — Informações adicionais. Isso se aplica somente a uma aprovação completa e não a itens individuais dentro de uma aprovação. A notificação deve vir acompanhada de uma cópia da notificação de fim de vida enviada pelo vendedor aos seus clientes. O(s) produto(s) continuará(ão) a ser listado pela PCI conforme aprovado até a data de expiração da aprovação natural com notação da cessação de vendas do fornecedor para novas implantações, a menos que outros motivos (por exemplo, comprometimento do dispositivo) determinem a retirada da aprovação pela PCI. Em todos os casos, os fornecedores não terão permissão para manipular listagens de produtos para evitar a taxa de listagem ou de manutenção.

6 Processo de Aprovação

6.1 Acordo de liberação e entrega de relatório

Antes do laboratório divulgar o relatório de avaliação, o fornecedor deverá assinar um formulário de consentimento ou contrato de liberação de confidencialidade, dando permissão para a divulgação das informações para o PCI SSC para consideração de aprovação. Além disso, o fornecedor deve assinar o *Acordo de Liberação do Fornecedor da Indústria de cartões de pagamento*, que é enviado pelo laboratório de teste junto com o relatório. Para serem aceitos para consideração de aprovação do dispositivo de segurança de pagamento, os relatórios de avaliação do dispositivo de segurança de pagamento**devem ser entregues diretamente** ao PCI SSC pelos laboratórios.

Para que o PCI SSC revise qualquer relatório de avaliação para listagem no Site, o Fornecedor deve fornecer uma cópia assinada do Contrato de Liberação do Fornecedor (VRA) atual para o Laboratório PTS. A versão atual do VRA está disponível no site público.

Os fornecedores ou outros terceiros que estiverem licenciando produtos aprovados de outros fornecedores para comercializar ou distribuir sob seus próprios nomes, também devem assinar um contrato de liberação do fornecedor antes da emissão da aprovação.

Referências no contrato de liberação do fornecedor a “TPP” ou “Produto de Terceiros” não se aplicam aos deltas para aprovações que existiam antes da assinatura do Contrato de Liberação do Fornecedor pelo fornecedor com essa referência. Isso se aplica a todas as novas aprovações subsequentes que resultem em um novo número de aprovação e deltas dessas mesmas homologações.

Em todos os casos, o Contrato de Liberação do Fornecedor, a menos que substituído ou rescindido de outra forma, de acordo com as disposições do contrato, exigirá somente um único envio para cobrir todos os produtos enviados dos fornecedores.

6.2 Funções e responsabilidades

A responsabilidade e a autoridade do laboratório são limitadas ao desempenho dos testes de dispositivos de segurança de pagamento e à geração de um relatório de avaliação que descreve os resultados dos testes. É de responsabilidade e autoridade do PCI SSC considerar um dispositivo de segurança de pagamento para aprovação com base nos resultados relatados pelo laboratório.

É de responsabilidade do Laboratório e do Fornecedor permitir tempo suficiente no agendamento do projeto: avaliação do dispositivo, envio de relatórios para revisão, respostas de consultas e reenvios de relatórios, processo de aprovação, etc.

6.3 Emissão de aprovação

O PCI SSC baseará sua aprovação somente nos resultados do relatório de avaliação laboratorial. Todos os relatórios, consultas de revisores de relatórios e respostas de Laboratórios a consultas são gerenciados por meio do Portal do PCI SSC. Após receber o relatório de teste para uma nova avaliação, o PCI SSC tem duas semanas (14 dias corridos) a partir do recebimento desse relatório para identificar quaisquer problemas técnicos ou questões a serem resolvidas pelo laboratório de testes. Se o relatório for considerado como suficientemente deficiente em qualidade pelos revisores, será rejeitado antes de ser revisto na sua totalidade e deverá ser refeito pelo laboratório e reenviado, o que reiniciará todo o processo.

Se os problemas ou as perguntas para o laboratório não forem identificados dentro deste prazo, o PCI SSC deverá publicar as informações de aprovação no site e emitir uma carta de aprovação. Se forem identificadas dúvidas ou problemas e enviados para o laboratório, o ciclo será redefinido para uma semana (sete dias corridos) após a recepção de uma resposta completa e aceitável do laboratório. O começo da redefinição de sete dias não ocorrerá até o recebimento de uma resposta aceitável para o último item aberto previamente identificado. Em caso de dúvidas ou problemas adicionais, o ciclo se repete até que uma resposta satisfatória seja recebida, momento em que o PCI SSC publicará as informações no site do PCI SSC e emitirá a carta de aprovação. Em todos os casos em que os relatórios exigirem o reenvio como parte do processo de tratamento de questões técnicas ou perguntas, as alterações em todos os relatórios subsequentes ao relatório inicial deverão ser feitas com marcas de revisão, ou seja, "sublinhadas em vermelho".

Questões adicionais ou questões que são levantadas além do período inicial de 14 dias limitam-se à mesma área de segurança para a qual as questões técnicas ou questões foram originalmente geradas. Em geral, isso significa limitar-se ao(s) mesmo(s) requisito(s) de segurança; no entanto, as informações fornecidas pelo laboratório de ensaio podem afetar outros requisitos de segurança, o que, por conseguinte, seria abrangido.

No caso de relatórios sobre modificações nos dispositivos aprovados existentes, denominados letras ou relatórios "delta", o ciclo (por exemplo, 14 dias corridos iniciais) é o mesmo, e o PCI SSC deve publicar as informações revistas no site e emitir uma carta de aprovação revista, a menos que surjam problemas ou dúvidas de maneira semelhante ao acima mencionado. Os relatórios Delta são preparados com os principais requisitos com os quais o dispositivo de segurança de pagamento foi avaliado quando recém-aprovado. Quando possível, as alterações atribuídas ao delta devem usar marcas de revisão no relatório original. Se não for possível,—por exemplo, devido a inúmeros deltas no mesmo dispositivo,—as alterações ainda devem ser explicitamente observadas.

Em todos os casos, podem ser emitidas cartas de aprovação mais cedo se todas as marcas de pagamento se afirmarem de forma positiva.

A carta de aprovação e listagem da PCI em www.pcisecuritystandards.org conterá, no mínimo, as seguintes informações. Cada característica está detalhada no Apêndice A, "Lista de dispositivos no site PCI SSC*".*

- Identificador de dispositivo de segurança de pagamento
- Número de aprovação
- Tipo de produto
- Classe de aprovação
- Versão
- Data de vencimento
- Suporte para PIN (online, offline) — somente POI
- Gerenciamento de Chaves — somente POI
- Controle de aviso
- Funções fornecidas
- Componentes aprovados

***Observação**:*
O PCI SSC não concederá nenhuma "aprovação parcial" com base na capacidade de um dispositivo PTS de atender a alguns, mas não todos, os requisitos de segurança físicos ou lógicos necessários e aplicáveis

Por vários motivos, incluindo a revogação da aprovação, as informações sobre cartas de aprovação podem tornar-se imprecisas. Portanto, o site da PCI é considerado a fonte autorizada e deve sempre ser usado para validar o status de aprovação do produto de um fornecedor.

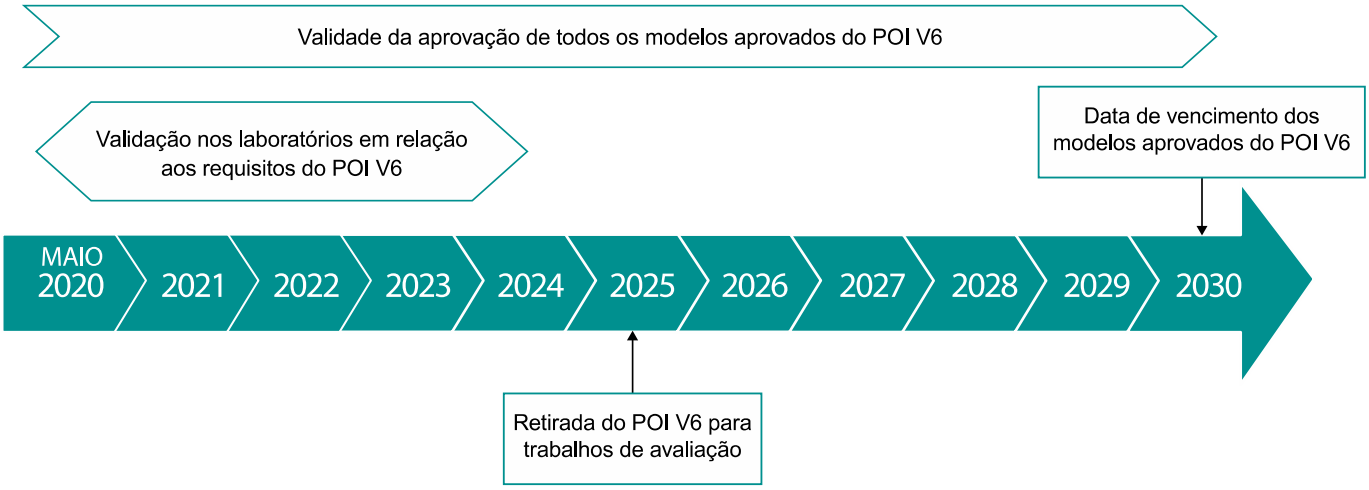
6.4 Atraso de listagem

Os fornecedores podem optar por atrasar a listagem de um dispositivo recém-aprovado por até um máximo de seis meses. A notificação por escrito ao PCI SSC deve ser enviada por meio do laboratório aplicável, junto com o relatório de avaliação. Além disso, o laboratório deve fazer uma anotação na seção “Observações” do portal de relatórios do laboratório indicando o período pelo qual a listagem do dispositivo deve ser retida.

6.5 Expiração da aprovação

Para manter a aprovação de um determinado modelo aprovado, o fornecedor deve ter o modelo de dispositivo aprovado reavaliado em relação à versão atual do padrão de PTS da PCI antes da data de expiração, conforme apresentado na lista de aprovações de PTS da PCI. Após a conclusão bem-sucedida, uma nova aprovação será emitida sob a versão principal aplicável dos requisitos.

O seguinte diagrama mostra a relação entre a expiração do modelo de dispositivo testado na Versão 6 dos Requisitos de Segurança de POI de PTS da PCI e seu trabalho de testes em laboratório.



Para os dispositivos que incorporam outros dispositivos aprovados pela PCI e, portanto, baseiam a sua segurança nesses subcomponentes (mesmo parcialmente), a data de validade deve ser a mais antiga a expirar entre todas as avaliações, inclusive o próprio dispositivo integrado.

7 Alterações a um Dispositivo PTS Previamente Aprovado

Se um dispositivo desegurança de pagamento aprovado tiver passado por alterações que podem afetar a segurança e/ou se o fornecedor desejar as informações em sua *Carta de Aprovação de POI* ou *Carta de Aprovação* de HSM e no site revisa do da PCI, o fornecedor deve enviar documentação de alteração adequada ao laboratório para determinar se uma avaliação completa precisa ser realizada. O laboratório comunicará ao PCI SSC qualquer informação sobre alterações a um dispositivo de segurança de pagamento previamente aprovado. O PCI SSC indicará as atualizações em conformidade em sua *Carta de Aprovação*revisada e no site do PCI SSC, www.pcisecuritystandards.org.

Observação:

Se os fornecedores de dispositivos de segurança de pagamento puderem modularizar a funcionalidade do dispositivo de segurança de pagamento, isso ajudaria a minimizar as reavaliações devido a alterações de hardware que não afetam a segurança do dispositivo de segurança de pagamento.

7.1 Manutenção da aprovação

1. **Nenhum impacto nos requisitos de segurança: não é necessário um novo teste para manter a aprovação**

   Se o hardware ou o firmware (incluindo o software que impactar a segurança) do dispositivo de segurança de pagamento previamente aprovado for revisto, mas essa revisão for considerada menor e não impactar negativamente a segurança, a documentação da alteração poderá ser enviada ao laboratório para revisão. É altamente recomendável que o fornecedor use o mesmo laboratório utilizado para a avaliação original.

   Quando adequado, o laboratório emitirá uma carta ao PCI SSC descrevendo a natureza da alteração, indicando que não afeta a conformidade dos POIs ou do HSMs com os requisitos de segurança PCI. O PCI SSC então analisará a carta para determinar se a alteração tem algum impacto no status de aprovação do dispositivo de segurança de pagamento.

   Supondo-se que não houvesse impacto, o novo número de versão de hardware e/ou firmware seria considerado “Aprovado” e:

   - A lista de dispositivos de segurança de pagamento aprovada no site da PCI seria atualizada de acordo com as novas informações, e
   - Uma carta revisada de aprovação será emitida ao fornecedor.

2. **Possível impacto nos requisitos de segurança: são necessários novos testes para manter a aprovação**

   Se as mudanças no dispositivo afetarem os requisitos de segurança do dispositivo de segurança de pagamento, o dispositivo deverá ser submetido a outra avaliação de segurança. O laboratório apresentará então um novo relatório de avaliação ao PCI SSC para análise de nova aprovação. Em tal cenário, o fornecedor deve primeiro enviar a documentação da alteração ao laboratório, o que determinará se a natureza da alteração afeta a segurança do dispositivo de segurança de pagamentos, de acordo com os requisitos atuais de segurança do dispositivo de segurança de pagamentos da PCI.

7.2 Limite da aprovação

O limite da aprovação por meio da qual uma aprovação de um modelo de dispositivo de segurança de pagamento existente pode ser levada para um novo modelo de dispositivo de segurança de pagamento (ou similar) pode ser obtido do seguinte modo:

1. O fornecedor descreve o projeto do novo modelo de dispositivo de segurança de pagamento (ou similar) na forma de um documento de revisão do produto.
2. O fornecedor manda a documentação para o laboratório selecionado para revisão.
3. O laboratório faz a análise da documentação (e possivelmente das amostras de dispositivos de segurança de pagamento).
4. O laboratório trata o processo de revisão de documentos como revisão do produto de um dispositivo de segurança de pagamento aprovado existente.
5. O laboratório então envia uma carta ao fornecedor informando se uma avaliação completa do teste será ou não necessária.

7.3 Dispositivos compostos

Os dispositivos compostos, como terminais de pagamento autônomos, podem ser avaliados como parte de uma única avaliação de todos os componentes aplicáveis ou podem ser avaliados com um ou mais componentes OEM previamente aprovados. Se um dispositivo composto incorporar componentes aprovados previamente, as seguintes considerações para a avaliação devem ser feitas:

- Os relatórios de avaliação UPT contendo componentes OEM aprovados em separado devem conter no mínimo uma tabela resumida de todos os requisitos (sim ou N/D) de qualquer módulo que for relevante para o fator de forma final da UPT. Essa tabela pode fazer referência ao componente OEM pertinente para conformidade com qualquer requisito específico.
- Todos os requisitos afetados (por exemplo, mecanismos adicionais de entrada de titulares de cartões, monitores, controladores, etc.) pelo formato final da UPT devem ser abordados em pormenor para cada requisito afetado.
- Se o laboratório que avalia o formato final não for o mesmo laboratório que avaliou os componentes OEM, o laboratório deverá ter acesso ao(s) relatório(s) de laboratório de componentes OEM. Se esses relatórios não estiverem disponíveis, por exemplo, porque os fornecedores de envio são diferentes ou por qualquer outra restrição, o laboratório deve determinar a extensão do trabalho adicional necessário.
- Se o laboratório não puder confiar nas informações disponíveis nos relatórios que não estiverem disponíveis para o laboratório, e o laboratório não puder executar o grau de trabalho adicional necessário para alcançar tal dependência, eles deverão recusar o envolvimento.
- Em todos os casos, o PCI SSC pode rejeitar o relatório se, na avaliação do PCI SSC, o relatório não contiver informações adequadas para fundamentar as conclusões do cumprimento dos critérios globais de UPT.

Os componentes OEM aprovados contra requisitos de segurança anteriores somente são permitidos para uso na obtenção de uma avaliação global de aprovação UPT sem testes adicionais desses componentes se não forem mais do que uma versão principal dos requisitos anteriormente. Exemplo, os EPPs avaliados e aprovados com POI da PCI v5.x podem ser usados sem testes adicionais de requisitos que atenderam anteriormente como parte de uma avaliação geral do POI v6. Contudo, os EPPs que foram avaliados e aprovados com EPP da PCI v4.x devem ser submetidos a uma avaliação completa de acordo com todos os requisitos de POI v6 aplicáveis.

Os requisitos adicionais de segurança individuais constantes das POI v6 que não tenham sido previamente avaliados continuam a ser aplicados, se aplicável, à avaliação global da UPT. Além disso, para os dispositivos que incorporam outros dispositivos aprovados pela PCI e, portanto, baseiam a sua segurança nesses subcomponentes (mesmo parcialmente), a data de validade deve ser a mais antiga a expirar entre todas as avaliações, incluindo o próprio dispositivo integrado.

7.4 Rebranding/Licenciamento

Fornecedores ou outros terceiros que licenciam produtos aprovados de outros fornecedores para comercializar ou distribuir sob seus próprios nomes não são obrigados a pagar uma nova taxa de avaliação se a única alteração for na placa de identificação. Se forem feitas alterações de firmware ou de hardware que exigirem um laboratório de ensaio reconhecido pela PCI para avaliar as alterações em relação ao impacto potencial na segurança, o licenciado deverá pagar a nova taxa de avaliação. Em todos os casos, o dispositivo licenciado receberá um novo número de aprovação, e o fornecedor do licenciado ou terceiro pagará a taxa anual de listagem para cada aprovação.

Considerações adicionais para um terceiro licenciar um produto aprovado de um fornecedor, onde o terceiro deseja distribuí-lo como seu próprio produto são:

1. O fornecedor do licenciado não pode solicitar diretamente. O fornecedor licenciante deve solicitar em seu nome.
2. Todas essas solicitações devem ser recebidas pelo PCI SSC como uma carta delta de um dos laboratórios reconhecidos de PTS do PCI SSC. Se a única mudança for para a placa de identificação do produto, não há uma nova taxa de avaliação mas, como mencionado acima, haverá uma taxa de listagem anual.
3. Não há nenhuma exigência para que a versão do produto do licenciado faça referência ou liste o fornecedor original.
4. Os produtos podem ser licenciados por outro fornecedor, mesmo que a versão dos requisitos de segurança contra os quais o produto original foi aprovado seja retirado do uso para novas avaliações, desde que a aprovação não tenha expirado.
5. Como observado, produtos licenciados que requerem alterações físicas e/ou lógicas incorrerão em uma nova taxa de avaliação. Contudo, enquanto o fornecedor original continuar a fabricação do dispositivo em nome do fornecedor licenciado, o produto licenciado pode ser avaliado de acordo com a versão do requisito de segurança contra a qual o produto original foi avaliado e aprovado, mesmo que esses requisitos possam ser expirados para novos aprovações.
6. Se o fornecedor licenciado pretender fabricar diretamente o produto licenciado ou ter um terceiro que não o fornecedor original fabricando o produto licenciado em seu nome, o produto deve ser reavaliado como uma nova avaliação em relação à versão atual dos requisitos de segurança — a menos que o fornecedor licenciante possa demonstrar que mantém a propriedade intelectual e o controle de engenharia. Isto se deve ao potencial de mudanças nos plásticos, etc. que podem afetar a segurança do dispositivo.

Os fornecedores que estiverem em busca de várias listagens de aprovação separadas para seus próprios produtos estão sujeitos às mesmas condições para os itens 2, 3, 4 e 5, conforme aplicável.

Os fornecedores podem também criar dispositivos que se destinam somente a serem vendidos e/ou fabricados por outros fornecedores. Esses dispositivos podem ser avaliados e listados, ainda que o fornecedor original nunca possa vender esses dispositivos diretamente. Estes dispositivos podem ser avaliados e listados desde que os seguintes critérios sejam atendidos:

- O dispositivo deve ser totalmente capaz de executar a sua funcionalidade pretendida para a classe de homologação que é avaliada e pode ser vendido como um produto totalmente funcional. Isto não impede o dispositivo que solicitar software adicional, como aplicativos de pagamento, mas o firmware do dispositivo deve atender a todos os requisitos aplicáveis.
- O dispositivo deve ter sua própria avaliação e listagem de produtos,
- Cada um dos segundos fornecedores que utilizam o projeto do dispositivo e/ou fabricar o dispositivo deve ter sua própria avaliação completa (NÃO UM DELTA) e listagem separada.

Os dispositivos que exigem hardware e/ou firmware adicionais para operar (como componentes individuais) não poderiam ser avaliados. Esses componentes devem ser integrados em um projeto de dispositivo que atenda aos requisitos exigidos de PTS (HSM ou POI).

7.5 Retirada de aprovação

Os fornecedores podem enviar uma solicitação para a retirada por escrito pelo PCI SSC de uma aprovação em que o fornecedor nunca tenha vendido ou implantado qualquer dispositivo de um modelo específico previamente aprovado. Isso se aplica somente a uma aprovação completa e não a itens individuais dentro de uma aprovação. O pedido deve ser feito com o formulário Solicitação De Alteração Administrativa de PTS por meio de um dos laboratórios de teste reconhecidos pela PCI. Tal formulário está disponível por meio dos laboratórios ou do gerente do programa de PTS pcipts@pcisecuritystandards.org.

7.6 Alterações administrativas

Os fornecedores que sofreram uma alteração de nome legal e desejam que suas listagens de aprovação sejam atualizadas em conformidade, devem enviar um formulário de solicitação de alteração administrativa do PTS por meio de um laboratório de teste reconhecido pelo PTS. O fornecedor deve também enviar um novo Contrato de Liberação do Fornecedor sob o novo nome da empresa. Se a aparência do dispositivo for alterada para refletir um novo nome (rótulos ou placa frontal), um relatório delta deverá ser emitido por meio de um dos laboratórios.

Os fornecedores que querem alterar um nome de modelo de um dispositivo aprovado também devem usar o formulário Solicitação de alteração administrativa de PTS. No entanto, se algum dispositivo tiver sido vendido sob o nome do modelo anterior, ambos os nomes serão listados. Além disso, uma nova política de segurança deve ser criada e deve fazer referência aos nomes novos e antigos, ou então será listada em paralelo à política existente. Além disso, as imagens para o dispositivo usado no site www.pcisecuritystandards.org devem incluir os modelos anteriores e novos.

8 Notificação após uma violação ou um comprometimento de segurança

Os fornecedores devem notificar o PCI SSC sobre qualquer violação ou comprometimento de segurança que ocorrer em relação a um dispositivo de segurança de pagamento aprovado, empregando os procedimentos descritos nesta seção.

8.1 Notificação e tempo

Não obstante quaisquer outras obrigações legais que o fornecedor possa ter, o fornecedor deve notificar imediatamente o PCI Security Standards Council (Conselho de Padrões de Segurança da PCI, “Conselho”) de qualquer violação ou comprometimento de segurança relacionado a qualquer fornecedor que tenha fornecido:

- Ponto de interação ou módulo de segurança de hardware
- Instalação de geração de chaves
- Instalação de carregamento de chaves

O fornecedor também deve enviar informações imediatas sobre qualquer possível impacto que essa violação (possível ou real) possa ter ou terá.

Observação:

A notificação deve ocorrer o mais tardar 24 horas após o fornecedor descobrir a violação ou comprometimento de segurança.

8.2 Formato da notificação

A notificação inicial do fornecedor de uma violação ou comprometimento de segurança deve se dar na forma de uma chamada telefônica para o PCI SSC para o número +1-781-876-8855 (opção 3, selecione "Programa PIN ”), seguido por um e-mail (pcipts@pcisecuritystandards.org) apresentando os detalhes completos sobre a violação ou o comprometimento de segurança.

8.3 Detalhes da notificação

Depois de notificar uma violação ou comprometimento de segurança, o fornecedor deve fornecer ao PCI SSC todas as informações relevantes relacionadas a essa violação ou comprometimento de segurança. Isso inclui, entre outros:

- O número e a localização dos produtos reais afetados
- O número das contas comprometidas (se conhecido)
- Detalhes de quaisquer chaves comprometidas
- Quaisquer relatórios que descrevam a violação ou o comprometimento de segurança
- Quaisquer relatórios ou avaliações executadas para investigar a violação ou o comprometimento de segurança

O PCI SSC, conforme acordado nos termos do *Contrato de liberação do fornecedor da indústria de cartões de pagamentos,* pode compartilhar essas informações com laboratórios reconhecidos pela PCI para permitir uma avaliação da violação ou do comprometimento de segurança a ser realizada para mitigar ou evitar novas violações ou comprometimentos de segurança. Como resultado dessa notificação, o PCI SSC trabalhará com o fornecedor para corrigir todas vulnerabilidades de segurança e produzirá um documento de diretriz a ser emitido aos clientes desse fornecedor, informando-os sobre todas as possíveis vulnerabilidades e detalhando quais ações devem ser tomadas para mitigar ou evitar outras violações ou comprometimento de segurança.

8.4 Ação após uma violação ou um comprometimento de segurança

No caso de o PCI SSC estar ciente de uma fraqueza de segurança ou comprometimento real relacionado a um produto específico ou grupo de produtos aprovados, o PCI SSC tomará as seguintes providências:

- Notificar os participantes da bandeira de pagamento da PCI de que ocorreu uma fraqueza ou um comprometimento de segurança.
- Tentar obter o terminal comprometido para avaliar exatamente como o comprometimento ocorreu. Isto pode envolver a utilização laboratórios reconhecidos pela PCI.
- Entre em contato com o fornecedor para informá-lo de que o produto tem uma fraqueza de segurança ou foi comprometido e, sempre que possível, envie informações relacionadas com a verdadeira fraqueza ou comprometimento.
- Trabalhe com o fornecedor para tentar mitigar ou evitar outros comprometimentos.
- Trabalhe com as agências oficiais apropriadas para ajudar a mitigar ou evitar novos comprometimentos.
- Faça avaliações do produto comprometido, seja internamente ou sob os termos do *Contrato de liberação do fornecedor da indústria de cartões de pagamento* , utilizando laboratórios reconhecidos pela PCI para identificar a causa do comprometimento.

8.5 Retirada da aprovação

O PCI SSC reserva-se o direito de retirar a aprovação de um dispositivo de POI ou HSM e, consequentemente, atualizar a *Lista de aprovação de dispositivos PCI PTS.* Algumas das razões para a retirada da aprovação são:

- É claro que o dispositivo de segurança de pagamento não oferece proteção suficiente contra ameaças atuais e não se encontra em conformidade com os requisitos de segurança. Se o PCI SSC considerar que o dispositivo de segurança de pagamento tem uma fraqueza de segurança ou foi comprometido, o PCI SSC notificará o fornecedor por escrito sobre sua intenção de retirar sua aprovação para esse dispositivo de segurança de pagamento.
- O fornecedor não cumpre obrigações contratuais em relação ao PCI SSC ou rigorosamente segue os termos de participação no programa PCI PTS conforme descrito neste documento ou no *Contrato de Liberação do Fornecedor da Indústria de cartões de pagamento.*

9 Termos e condições legais

A aprovação do PCI SSC se aplica apenas a dispositivos de segurança de pagamento idênticos ao dispositivo de segurança de pagamento testado por um laboratório reconhecido pelo PCI Security Standards Council. Se qualquer aspecto do dispositivo de segurança de pagamento diferir do que foi testado pelo laboratório, mesmo que o dispositivo de segurança de pagamento esteja em conformidade com a descrição básica do produto contida na carta de aprovação, o modelo do dispositivo de segurança de pagamento não deverá ser considerado aprovado nem promovido como aprovado. Por exemplo, se um dispositivo de segurança de pagamento apresentar firmware, software ou construção física com o mesmo nome ou número de modelo que os testados pelo laboratório, mas na realidade não for idêntico às amostras de dispositivos de segurança de pagamento testadas pelo laboratório, o dispositivo de segurança de pagamento não deverá ser considerado nem promovido como aprovado.

Nenhum fornecedor ou outro terceiro pode se referir a um dispositivo de segurança de pagamento como “Aprovado pela PCI”, ou de outra forma declarar ou implicar que o PCI SSC tenha, no todo ou em parte, aprovado qualquer aspecto de um fornecedor ou seus dispositivos de segurança de pagamento, exceto na medida e sujeito aos termos e restrições expressamente estabelecidos por escrito acordo com o PCI SSC, ou em uma carta de aprovação. Todas as outras referências à aprovação do PCI SSC são estrita e ativamente proibidas pelo PCI SSC.

Se concedida, a aprovação é concedida pelo PCI SSC para garantir certas características operacionais e de segurança importantes para a realização dos objetivos do PCI SSC, mas a aprovação não representa, em nenhuma circunstância, qualquer endosso ou garantia em relação à funcionalidade, à qualidade ou ao desempenho de qualquer produto ou serviço específico. O PCI SSC não garante nenhum produto ou serviço oferecido por terceiros. A aprovação não inclui, sob nenhuma circunstância, nem implica em qualquer garantia de produto do PCI SSC, incluindo, entre outros, quaisquer garantias implícitas de comercialização, adequação ao propósito ou não violação, todas as quais são expressamente renunciadas pelo PCI SSC. Todos os direitos e recursos relativos a produtos e serviços, que tenham recebido uma aprovação, serão fornecidos pela parte que fornece esses produtos ou serviços, e não pelo PCI SSC ou pelos participantes da bandeira de pagamento.

10 Glossário de termos e acrônimos

Termo	Definição
Classe de Aprovação	A classe de aprovação descreve com que requisitos de avaliação o dispositivo aprovado foi testado. Ver o Apêndice A.
COTS	Dispositivo disponível comercialmente. Um dispositivo móvel (por exemplo, smartphone ou tablet) projetado para distribuição no mercado em massa e que não foi projetado especificamente para processamento de pagamentos.
CTLS	Sem contato
Dispositivo	Dispositivo de pagamento; pode ser parte de um terminal.
EPP	Teclado de PIN criptografado; classe de aprovação, designando dispositivos incorporáveis (OEM) a serem integrados em um terminal operado pelo titular do cartão. Ver o Apêndice A.
Estrutura de avaliação	Conjunto de requisitos para fornecedores, metodologia de testes para laboratórios, processo de aprovação para produtos e lista de aprovação referente a um determinado tipo de dispositivo de segurança de pagamento (dispositivo de POI, HSM).
HSM	Módulo de segurança de hardware; classe de aprovação destinada a dispositivos compatíveis com uma variedade de aplicativos e processos de processamento de pagamento e autenticação de titulares de cartão. Ver o Apêndice A.
Leitor híbrido	Dispositivo que incorpora recursos de captura de dados do cartão, seja um cartão de faixa magnética ou de circuito integrado (também conhecido como cartão inteligente ou de chip).
ICCR	Leitor de cartão com circuito integrado
KLD	Dispositivo de carregamento de chave
MSR	Leitor de tarja magnética
OEM	Fabricante do equipamento original
Dispositivo de segurança de pagamentos	Qualquer dispositivo completo (por exemplo, um dispositivo de aceitação de PIN voltado para o consumidor ou um HSM) cujas características contribuem para a segurança de pagamentos eletrônicos de varejo ou outras transações financeiras.
Programa de avaliação de segurança de dispositivos de PTS da PCI	A estrutura de avaliação do PCI SSC para dispositivos de sistema de pagamento.

Termo	Definição
PED	Dispositivo de entrada de PIN; classe de aprovação destinada a dispositivos de entrada de PIN e capacidade de processamento de PIN, atendidos ou autônomos, cujo objetivo principal é capturar e transmitir o PIN para um leitor ICC e/ou para outro dispositivo de processamento, como um sistema host. Um PED deve ter uma tela integrada, a menos que seja dedicado somente à entrada de PIN. Ver o Apêndice A.
POI	Ponto de interação
dispositivos de POI	Dispositivo utilizado no ponto de interação com um consumidor.
Tipo de produto	O tipo de produto descreve tanto a classe de aprovação de um dispositivo quanto se o dispositivo é um módulo a ser integrado (OEM) ou não.
PTS	segurança em transações com PIN, a estrutura do PCI SSC para dispositivos de segurança de pagamento. Refere-se coletivamente a dispositivos de POI e HSMs.
Dispositivos PTS	Dispositivos de segurança de pagamento, dispositivos de POI e HSMs.
PTS-HSM	A subestrutura da estrutura de segurança do dispositivo PCI-PTS que aborda a segurança de HSMs.
PTS-POI	A subestrutura da estrutura de segurança do dispositivo PCI-PTS que aborda a segurança dos dispositivos voltados para o consumidor.
RAP	Plataforma de administração remota para HSMs
SCR	Classe de aprovação do leitor de cartão seguro
SCRP	Classe de aprovação do PIN do leitor de cartão seguro
SPoC	Entrada de PIN baseada em software em COTS
SRED	Leitura segura e intercâmbio de dados
Terminal	Dispositivo comercial com uma função de negócios. Pode ser dedicado a pagamentos (terminal de PDV com um teclado de PIN integrado ou separado) ou à distribuição de produtos (como um caixa automático ou uma bomba de combustível de autosserviço).
Ciclo de teste	Conclusão de todos os procedimentos aplicáveis de teste realizados em uma única versão do dispositivo de segurança de pagamento do fornecedor.
UPT	Terminal de pagamento autônomo; classe de aprovação, dispositivos de pagamento operados por portadores de cartão (autosserviço) que leem, capturam e transmitem informações do cartão em conjunto com um dispositivo de autoatendimento autônomo. Ver o Apêndice A.

Apêndice A: lista de dispositivos no site do PCI SSC

Veja abaixo as características de uma listagem de dispositivos no site do PCI SSC.

A.1 Ponto de interação (POI)

Para os fins destes requisitos, um **dispositivo de aceitação de PIN em POI** é definido como:

> *Um dispositivo que prevê a entrada de PINs, utilizado para a compra de bens ou serviços ou liberação de dinheiro. Um POI aprovado atendeu a todos os requisitos de POI para PTS da PCI aplicáveis à entrada de PIN online e/ou offline e tem um limite físico e lógico claramente definido para todas as funções relacionadas à entrada de PIN.*

Além disso, os dispositivos de POI que não aceitam PIN podem ser validados e aprovados se estiverem em conformidade com os requisitos de Leitura Segura e Intercâmbio de Dados (SRED) e, se aplicável, com os requisitos de protocolos abertos. Esses dispositivos devem ser explicitamente indicados como não aprovados para aceitação de PIN.

Leitores de cartões seguros e leitores de cartões seguros de PIN devem ser validados de acordo com os requisitos descritos no *Apêndice B: Aplicabilidade dos Requisitos* dos *Requisitos de Segurança modular de ponto de interação (POI) da Segurança de Transação com PIN (PTS).*

Todas as classes de aprovação estão sujeitas aos Requisitos de Segurança do ciclo de vida.

Um dispositivo de POI pode ser autônomo e não integrável, caso em que a classe de aprovação PED pode ser aplicável. Essa classe pode ser aplicada tanto a assistidos como a autônomos. Contudo, os fornecedores podem optar por listar um terminal autônomo sob a classe UPT ao atenderem aos requisitos apropriados.

Se o dispositivo de POI fosse projetado para ser incorporado em um conjunto mais amplo (por exemplo, máquina de venda automática ou caixa eletrônico), então a classe de aprovação EPP ou PED seria aplicada. Nesse caso, pode haver outras funcionalidades presentes além da captura e do transporte de PIN (por exemplo, tela, leitor de cartão). Os dispositivos que se encaixam nessa categoria terão a propriedade do tipo de produto prefixada com a palavra “OEM” na página principal da listagem, para anunciar inequivocamente a natureza modular.

Os dispositivos de POI que combinam a entrega de mercadorias (por exemplo, gasolina) ou serviços (máquina de bilhetes) com pagamento baseado em PIN estão qualificadas para a classe de aprovação UPT. Esses POI possivelmente podem conter módulos OEM aprovados.

Os dispositivos de POI enviados para testes devem ser devidamente identificados para que os clientes participantes da PCI ou seus agentes possam estar seguros de que estão adquirindo um POI aprovado pela PCI.

A.2 Módulos de segurança de hardware (HSM)

Para propósitos destes requisitos, um **HSM** é definido como:

> *Um dispositivo de hardware protegido física e logicamente que apresenta um conjunto seguro de serviços criptográficos. Ele inclui o conjunto de hardware, firmware, software, ou alguma combinação destes, que implementa lógica criptográfica, processos criptográficos, ou ambos, incluindo algoritmos criptográficos.*

Além disso, este documento apresenta uma estrutura de aprovação de duas camadas para HSMs. Esses níveis apresentam diferenças somente na seção Requisitos de Segurança Física, conforme delineado nos *Requisitos de teste derivado de HSM da PCI.*Os HSMs podem ser aprovados como projetados para uso em ambientes controlados, conforme definido na*norma ISO 13491-2: serviços bancários, dispositivos de criptografia segura (varejo)* ou aprovados para uso em qualquer ambiente operacional. Essas categorias são:

- **Restrito —** A aprovação é válida somente quando implantada em ambientes controlados ou mais robustos (por exemplo, ambientes seguros) conforme definido na ISO 13491-2 e na política de segurança de HSM da PCI para o dispositivo.
- **Irrestrito –** A aprovação é válida em qualquer ambiente.

A.3 Dispositivos com aprovação expirada

São dispositivos cuja aprovação já expirou conforme ressaltado na seção “Data de expiração” deste documento. Para obter informações específicas sobre os mandatos de uso da bandeira de pagamento dos dispositivos expirados, entre em contato com a(s) bandeira(s) de pagamento envolvidas.

A.4 Identificador de dispositivo

O identificador de dispositivo é usado pela PCI para denotar todas as informações relevantes representativas de um ponto de interação ou módulo de segurança de hardware aprovado, e consiste em:

- Nome do Fornecedor
- Nome/Número do Modelo
- N.º do hardware
- N.º do firmware
- N.º do aplicativo, se aplicável

O nome ou o número do modelo deve estar presente, visível e destacada no dispositivo e não fazer parte de uma cadeia de caracteres maior. O dispositivo deve apresentar os números da versão de hardware e de firmware de acordo com a aprovação do dispositivo, refletindo as informações da listagem pública da PCI de dispositivos aprovados. O número de hardware deve ser exibido em uma etiqueta fixada ao dispositivo e estar identificado de forma destacada como a versão de hardware, por exemplo, N.º de HW, HWID, etc. Os números de versão do firmware e do aplicativo e, opcionalmente, o número da versão do hardware, devem ser exibidos no visor ou impressos durante o início ou sob solicitação Isso inclui todos os requisitos de segurança tratados nos testes, inclusive SRED e protocolos abertos. Se a etiqueta da versão do hardware não estiver visível quando o dispositivo for instalado, como em um EPP em um caixa eletrônico, deverá haver outros meios para indicar o número da versão. Esse meio deverá estar ilustrado por meio de provas fotográficas apresentadas no relatório de avaliação.

Para garantir que o dispositivo de segurança de pagamento tenha recebido uma aprovação, os clientes adquirentes ou seus agentes designados são recomendados com veemência que devem comprar e implantar somente os modelos de dispositivos de segurança de pagamento com as informações que correspondam exatamente às designações dadas aos componentes do ponto de identificador de dispositivo de interação ou o identificador do módulo de segurança de hardware.

Tabela 3: Exemplo de um identificador de dispositivo (cinco componentes)

Componente	Descrição
Nome do fornecedor	Acme
Nome/Número do POI	PIN Pad 600
N.º de Hardware	NN-421-000-AB
N.º de Firmware	Versão 1.01
N.º de Aplicativo	PCI 4.53

O identificador do dispositivo será incluído na carta de aprovação e no site da PCI. Se um dispositivo de segurança de pagamento idêntico for usado em uma família de dispositivos, os fornecedores serão advertidos contra o uso de um número de hardware (veja abaixo) que possa restringir a aprovação apenas a esse modelo de dispositivo de segurança de pagamento.

A.5 Nome/número do modelo

O nome/número do modelo não pode conter caracteres variáveis. Todos os dispositivos em uma família de dispositivos que se destinem a ser comercializados sob o mesmo número de aprovação devem ser explicitamente nomeados, e imagens desses dispositivos apresentados tanto no relatório de avaliação como para exibição na lista de aprovações. O fornecedor não pode utilizar um nome de modelo idêntico para mais de um dispositivo aprovado sob uma determinada versão principal dos requisitos de segurança.

A.6 N.º de hardware

N.º do hardware representa o conjunto específico de componentes de hardware usado no dispositivo de segurança de pagamento aprovado. Os campos que compõem o n.º de hardware podem consistir em uma combinação de caracteres alfanuméricos fixos e variáveis. Caracteres variáveis não são permitidos para nenhuma característica física ou lógica do dispositivo que impactem a segurança. As características do dispositivo que afetam a segurança devem ser indicadas por meio de caracteres fixos. A utilização de caracteres variáveis deve ser validada pelo laboratório de testes de modo a não afetar a segurança.

Observação:
O número da versão do firmware também pode estar sujeito ao uso de variáveis de maneira coerente com os números de versão de hardware

Um "x" minúsculo é usado pela PCI para designar todos os campos variáveis. O “x” representa campos do n.º de hardware que o fornecedor pode alterar a qualquer momento para indicar outra configuração de dispositivo. Alguns exemplos: código de uso do país, código do cliente, interface de comunicação, cor do dispositivo, etc.

O(s) campo(s) "x" foi(foram) avaliado(s) pelo laboratório e pelo PCI SSC para não afetar os requisitos de segurança do POI ou HSM ou a aprovação do fornecedor. Para assegurar que o dispositivo de segurança de pagamentos tenha sido aprovado, os clientes adquirentes ou seus agentes designados são fortemente aconselhados a comprar e implantar somente os dispositivos de segurança de pagamento com o n.º de hardware cujos caracteres alfanuméricos fixos correspondam exatamente ao número de hardware representado na Lista de aprovação do dispositivo de PTS da PCI.

Observação:

Os fornecedores podem ter produzido dispositivos de segurança de pagamento com o mesmo nome/número de modelo (antes da validação de conformidade pelo laboratório) que não atendam aos requisitos de segurança do dispositivo de segurança de pagamento

As opções que não puderem ser um caractere variável incluem aquelas que pertencerem diretamente ao cumprimento dos requisitos de segurança. Por exemplo, há requisitos para leitores de faixa magnética (MSRs) e leitores de cartões de circuito integrado (ICCRs). Um caractere variável não pode ser utilizado para designar se um dispositivo contém um MSR ou um ICCR. Há um requisito para a dissuasão da observação visual dos valores de PIN à medida que estão sendo introduzidos pelo titular do cartão, que podem ser cumpridos por escudos de privacidade ou pelo ambiente instalado do dispositivo ou por uma combinação destes. Não é apropriado cobrir as opções com caracteres curingas se o dispositivo for compatível com mais de um meio de dissuasão de observação.

Se um dispositivo for compatível com SRED ou OP, algumas opções que puderem normalmente ser aceitáveis para identificação por uma variável curinga não seriam permitidas. Por exemplo, a inclusão de leitores sem contato ou a inclusão de diversos pacotes de comunicação. Nesses casos, as configurações específicas validadas laboratório reconhecido pelo PTS devem ser explicitamente observadas na aprovação.

Além disso, todas as opções curinga, tanto em matéria de segurança como não relevantes para a segurança, devem ser claramente definidas e documentadas quanto às opções disponíveis e às suas funções tanto no relatório de avaliação como na política de segurança.

Tabela 4: Exemplos do uso de n.º de hardware

N.º de Hardware do dispositivo de segurança de pagamento na lista de aprovação	Comentários
NN-421-000-AB	O Hardware n.º NN-421-000-AB do identificador de dispositivo não emprega o uso da variável "**x.**". Assim, o dispositivo de segurança de pagamento que está sendo implantado deve corresponder exatamente ao número do hardware para que o dispositivo PTS seja considerado um dispositivo de segurança de pagamento aprovado (componente de hardware).
NN-4**x**1-0**x**0-A**x**	Hardware n.º NN-4**x**1-0**x**0-A**x** do identificador do dispositivo faz uso da variável "**x**." Assim, o dispositivo de segurança de pagamento que está sendo implantado deve corresponder exatamente ao n.º de hardware exatamente na(s) posição(ões) onde não há "**x**."
N.º de hardware real de POI disponibilizado pelo fornecedor	**Comentários**
NN-421-090-AC	Se o site da PCI informa NN-421-000-AB como o n.º de hardware no identificador de dispositivo, o dispositivo de segurança de pagamento com o n.º de Hardware NN-421-090-AC **não pode** ser considerado um dispositivo de segurança de pagamento aprovado (componente de hardware). No entanto, se o site do PCI informar NN-4**x**1-0**x**0-A**x** como o n.º de hardware no identificador de dispositivo, então o dispositivo de segurança de pagamento com n.º de Hardware NN-421-090-AC**poderá** ser considerado um dispositivo de segurança de pagamento aprovado (componente de hardware).
NN-421-090-YC	Se o site PCI informar NN-4**x**1-0**x**0-A**x** como o n.º de hardware no identificador de dispositivo, então o dispositivo de segurança de pagamento com o n.º de hardware NN-421-090-YC **não poderá** ser considerado um dispositivo de segurança de pagamento aprovado (componente de hardware).

A.7 Política de segurança

O fornecedor de dispositivos disponibiliza uma política de segurança disponível para o usuário, que trata do uso adequado do dispositivo de forma segura, incluindo informações sobre responsabilidades de gerenciamento de chaves, responsabilidades administrativas, funcionalidade do dispositivo, identificação e requisitos ambientais. A política de segurança deve definir as funções suportadas pelo dispositivo e indicar os serviços disponíveis para cada função em um formato tabular determinístico. O dispositivo tem a capacidade de executar somente suas funções projetadas, ou seja, não há nenhuma funcionalidade oculta. As únicas funções aprovadas que são executadas pelo dispositivo são aquelas permitidas pela política.

A.8 Número de aprovação

Os números de aprovação são atribuídos pelo PCI SSC no momento da aprovação e permanecem os mesmos durante a vida útil da aprovação do dispositivo.

A.9 Tipo de produto

O tipo de produto apresenta uma visão tanto da classe de aprovação de um dispositivo e se o dispositivo é um módulo a ser integrado (OEM) ou se está pronto para implantar equipamentos. O tipo do produto deve ser pré-fixado com **"OEM"** se o dispositivo aprovado for claramente concebido para ser integrado em um conjunto mais amplo, ou como um dispositivo diferente de PED para diferenciar claramente um dispositivo de POI sem aceitação de PIN de um dispositivo de POI para aceitação de PIN.

Fornecedores que fabricam produtos OEM autônomos do tipo módulo fixado ou encaixado, ou sejam, módulos PED totalmente funcionais que contêm todos os componentes necessários, para que os UPTs possam optar pela parceria com fornecedores de formato final desses UPTs (por exemplo, bombas de combustível automáticas ou fornecedores de quiosque). O produto do fornecedor OEM pode atender à maioria dos requisitos gerais de segurança UPT, e o fornecedor OEM pode enviar esse produto em conjunto com informações adicionais finais do fornecedor em nome desse fornecedor, como o projeto do AFD no caso de quiosque, ao laboratório para avaliação como UPT.

O produto do fornecedor OEM não pode receber aprovação UPT pois o produto do formato final real pode ter interfaces adicionais de titulares de cartões (por exemplo, monitores ou dispositivos de entrada de dados) ou outras características que estão dentro do escopo dos requisitos de segurança UPT. O formato final do produto do fornecedor receberá a aprovação UPT. O produto do fornecedor OEM receberia um número de aprovação separado e seria apresentado em separado; além disso, listado como um componente aprovado do produto UPT, semelhante à forma como outros produtos OEM são listados.

A.10 Classe de aprovação

A **Classe de Aprovação** é utilizada pela PCI para garantir que suas aprovações de dispositivos de segurança de pagamento descrevam com precisão projetos, arquiteturas e implementações em constante evolução atuais. Todos os POI e HSMs aprovados pelo PCI SSC na estrutura do Programa de avaliação de segurança de dispositivos de PTS da PCI, independentemente da classe de aprovação designada, têm o status de aprovação total da PCI. As instituições financeiras, ou seus agentes designados (por exemplo, comerciantes ou processadores), devem assegurar-se de que conhecem as diversas classes, pois representam como o dispositivo de segurança de pagamento atendeu aos requisitos de segurança do dispositivo de PTS da PCI.

Tabela 5: Descrições da classe de aprovação

Classe de aprovação	Descrição	Possíveis recursos *(veja a Tabela 7 abaixo para obter mais detalhes)*
EPP	Uma classe de aprovação que se destina a módulos seguros de entrada e de criptografia de PIN em um dispositivo de aceitação de PIN autônomo. Um EPP pode ter um monitor ou leitor de cartão incorporado ou pode utilizar monitores externos ou leitores de cartões instalados no dispositivo autônomo. Um EPP é tipicamente usado em um dispositivo autônomo de aceitação de PIN para a entrada do PIN e é controlado por um controlador de dispositivo. Um EPP tem um limite físico e lógico claramente definido e uma caixa inviolável/responsiva ou com violação evidente. No mínimo, um dispositivo enviado para aprovação de EPP deve conter um teclado numérico de entrada de PIN junto com seu módulo criptográfico seguro incorporado. Fabricantes de equipamentos originais (OEMs) ou fornecedores de criptografia de teclados de PIN (EPPs) para fabricantes de dispositivos de aceitação de PIN autônomos (por exemplo, caixas eletrônicos ou UPTs) e outros tipos de dispositivos de autoatendimento podem enviar apenas um EPP para testes laboratoriais e aprovação. Como parte integrante de um POI completo e totalmente funcional, um EPP OEM aprovado pode ser usado em outro dispositivo de pagamento, como um caixa eletrônico ou UPT para minimizar a redundância de testes. Contudo, os UPTs que utilizam um EPP aprovado continuarão a ser obrigados a passar por uma avaliação laboratorial, a fim de obter a aprovação global da UPT.	Tela Suporte para PIN Controle de aviso Gerenciamento de chaves Tecnologia de entrada de PIN ICCR MSR CTLS SRED OP

Classe de aprovação	Descrição	Possíveis recursos *(veja a Tabela 7 abaixo para obter mais detalhes)*
HSM	HSMs podem suportar uma variedade de aplicativos e processos de autenticação de titulares de cartões e processamentos de pagamentos. Os processos relevantes do conjunto total de requisitos descritos neste documento são: ▪ Processamento de PIN ▪ 3-D Seguro ▪ Verificação de cartão ▪ Produção e personalização de cartão ▪ EFTPOS ▪ Intercâmbio de caixa eletrônico ▪ Recarga de cartão de pagamentos ▪ Integridade de dados ▪ Processamento de transação com cartão com chip	N/A
KLD	Um SCD que possa ser utilizado para receber, armazenar e transferir dados com segurança entre equipamentos criptográficos e de comunicações compatíveis. As funções de transferência de chave e carregamento são as seguintes: ▪ Exportar de uma chave de um dispositivo criptográfico seguro (SCD) para outro SCD em texto simples, componente ou forma cifrada; ▪ Exportar de um componente chave de um SCD para um pacote inviolável (por exemplo, envelope de segurança); ▪ Importar de componentes chave para um SCD de um pacote inviolável; Armazenamento temporário da chave em texto simples, componente ou formulário cifrado dentro de um SCD durante a transferência.	N/A

Classe de aprovação	Descrição	Possíveis recursos *(veja a Tabela 7 abaixo para obter mais detalhes)*
Não-PED	Uma classe de aprovação de dispositivos de POI que NÃO permite a entrada de um PIN para uma transação de cartão de pagamento. Esta classe é para TODOS os dispositivos de POI ou combinações de dispositivos, atendidos ou autônomos, não compatíveis com transações de pagamento baseadas em PIN. Os tipos de produtos OEM podem exigir mais integração em um terminal POI. O dispositivo ou qualquer combinação de hardware pode ser utilizado conforme avaliado para operar em uma rede adquirente. O firmware deve incluir uma solicitação de pagamento aprovada pela adquirente necessária para o seu funcionamento. Os dispositivos de POI sem PED destinados ao uso em ambientes vigiados devem ser unidades autônomas e totalmente funcionais que possam processar transações de pagamento e devem conter uma interface comercial necessária para sua operação. Os dispositivos de POI (terminais) sem PED são validados pelos requisitos de leitura segura e intercâmbio de dados e, se aplicável, os requisitos de protocolos abertos. Esses dispositivos de POI sem PED NÃO são aprovados para a aceitação de PIN.	ICCR MSR CTLS SRED OP
PED	Uma classe de aprovação destinada a dispositivos de POI, que foi originalmente projetada para permitir o pagamento com entrada de PIN, e dedicada ao pagamento. Um PED deve ter uma tela integrada a menos que seja dedicado apenas à entrada de PIN. Esta classe pode cobrir ambientes atendidos e autônomos e OEM ou produtos autônomos.	Tela Recursos de PIN Controle de aviso Gerenciamento de chaves Tecnologia de entrada de PIN ICCR MSR CTLS SRED OP
RAP	Este é para plataformas utilizadas para a administração remota de HSMs. Tal administração pode incluir serviços de configuração do dispositivo e carregamento de chaves.	N/A

Classe de aprovação	Descrição	Possíveis recursos *(veja a Tabela 7 abaixo para obter mais detalhes)*
SCR	Um leitor de cartão criptografado que: ▪ Destina-se à utilização com um dispositivo não seguro, como um telefone celular ou outro dispositivo; ou ▪ Pode ser definido como um tipo de produto OEM a ser integrado em um terminal POI ou caixa eletrônico. Os tipos de produtos OEM podem conter um aplicativo de pagamento e ser capazes de uso autônomo ou podem ser dispositivos escravo para processar dados de conta de forma segura (SRED) e, se aplicável, realizar verificações de PIN offline e exigir conexão com um módulo, terminal ou bloco PIN seguro. O leitor de cartão seguro pode ser ▪ Um leitor de cartões híbridos ▪ Um leitor somente de tarjas magnéticas ▪ Um leitor somente de cartões com chip ▪ Um leitor somente de cartões sem contato Os SCRs devem atender, conforme o necessário, aos requisitos do ICCR e/ou MSR designados no Apêndice B dos*Requisitos de segurança de POI de PTS da PCI e os requisitos* de leitura segura e intercâmbio de dados. Se o dispositivo for capaz de se comunicar por meio de uma rede IP ou usar um protocolo de domínio público (como, entre outros, a Wi-Fi ou Bluetooth), os requisitos especificados nos requisitos de protocolos abertos também devem ser atendidos. Outros requisitos, como B1, Auto-testes e B9, números aleatórios, podem ser aplicados dependendo da funcionalidade do dispositivo. Se um SCR processar PINS, ou seja, se tiver recursos para autenticação de PIN offline por meio de um componente ICCR ou formatar e criptografar blocos de PIN para enviar online diretamente ao servidor, deverá ser validado em conjunto com um dispositivo de entrada PIN específico (por exemplo, PED ou EPP) para validar a segurança da interação, incluindo o estabelecimento da relação de chaveamento. O dispositivo de entrada de PIN deve ser previamente aprovado ou obter aprovação simultânea com o SCR no mesmo ou numa avaliação laboratorial simultânea e separada.	Recursos de PIN ICCR MSR CTLS SRED OP

Classe de aprovação	Descrição	Possíveis recursos *(veja a Tabela 7 abaixo para obter mais detalhes)*
SCRP	Um leitor de cartão de criptografia destinado a ser usado com um dispositivo comercialmente disponível (COTS), como um telefone celular ou tablet. Um PIN de leitor de cartão seguro (SCRP or SCR-PIN) pode ser: ▪ Um leitor de cartão de chip de contato ▪ Um leitor de cartão de chip sem contato ▪ Um leitor compatível com recursos de cartões com chip, com e sem contato ▪ Um leitor híbrido que contém um leitor de cartão de tarjas magnéticas e recursos de leitura de cartões com chipe com e sem contato Os SCRPs devem atender, como aplicável, aos requisitos do ICCR designados no Apêndice B dos requisitos de *segurança de de POI de PTS da PCI e os requisitos* de leitura segura e intercâmbio de dados. Se o dispositivo for capaz de se comunicar por meio de uma rede IP ou usar um protocolo de domínio público (como Wi-Fi ou Bluetooth, entre outros), deverá atender aos requisitos relevantes dos protocolos abertos. Outros requisitos nas seções física e lógica podem ser aplicados dependendo da funcionalidade do dispositivo. Os SCRPs fazem a tradução do PIN, dos PIN blocks recebidos do aplicativo de pagamento no dispositivo COTS, para um bloco de PIN para transporte para o host de processamento ou para verificação offline para o cartão de chip de contato.	Recursos de PIN Gerenciamento de chaves ICCR MSR CTLS SRED OP
UPT	A classe de dispositivo UPT cobre os dispositivos de pagamento operados pelo titular do cartão que leem, capturam e transmitem informações do cartão em conjunto com um dispositivo autosserviço autônomo, incluindo, entre outros, o seguinte: 1. Bomba de combustível automática 2. Máquina de bilhetes 3. Máquina de venda Os UPTs podem ter arquitetura composta, combinando diretamente o pagamento e a entrega de serviços e/ou bens.	Tela Recursos de PIN Controle de aviso Gerenciamento de chaves Tecnologia de entrada de PIN ICCR MSR CTLS SRED OP

A.11 Versão

A versão se refere à versão dos requisitos de segurança em que o dispositivo foi avaliado. Cada classe de aprovação pode seguir seu próprio cronograma de liberação.

A.12 Data de expiração

A data de expiração dos dispositivos aprovados pela PCI é a data em que a aprovação do dispositivo expira. Todas as aprovações de dispositivos expiram conforme o calendário abaixo, exceto para os SCRPs. Para os SCRPs, as aprovações expiram cinco anos após a data de aprovação.

Tabela 6: Datas de validade da aprovação

Versão dos Requisitos utilizada Durante a avaliação em laboratório	Requisitos de expiração	Expiração da aprovação dos modelos de dispositivos
Versão 6.x das *Solicitações de segurança de POI de PTS da PCI*	TBD 2024	Abril de 2030
Versão 5.x das *Solicitações de segurança de POI de PTS da PCI*	Junho de 2021	Abril de 2026
Versão 3.x das *Solicitações de segurança de HSM da PCI*	TBD 2021	Abril de 2026
Versão 4.x das *Solicitações de segurança de POI de PTS da PCI*	Setembro de 2017	Abril de 2023
Versão 2.x das *Solicitações de segurança de POI de PTS da PCI*	Junho de 2017	Abril de 2022
Versão 3.x das *Solicitações de segurança de POI de PTS da PCI*	Abril de 2014	Abril de 2021
Versão 1.x das *Solicitações de segurança de POI de PTS da PCI*	Abril de 2013	Abril de 2019
Versão 2.x das *Solicitações de segurança de PED ou EPP da PCI*	Abril de 2011	Abril de 2017
Versão 1.x das *Solicitações de segurança de UPT da PCI*	Abril de 2011	Abril de 2017
Versão 1.x *Solicitações de segurança de PED da PCI* ou *EPP*	Abril de 2008	Abril de 2014

As aprovações dos dispositivos avaliados pela PCI expiram seis anos depois da data efetiva de uma atualização subsequente dos requisitos de segurança da PCI.

O firmware POI v6 expira em três anos após a data de aprovação, mas não deve expirar após a expiração geral da aprovação do dispositivo.

A.13 Recursos específicos por classe de aprovação

Tabela 7: recursos específicos

Recurso e aplicabilidade	Descrição
Recursos de PIN (PED, EPP, SCR, SCRP, UPT)	**"Recursos de PIN"** indica o tipo de verificação de entrada de PIN possível no POI. "Online" representa que o POI oferece recursos para a verificação de PIN online pelo emissor do cartão de pagamento ou seu processador designado. Para aprovação nos testes, POIs com recursos de entrada de PIN online devem ser compatíveis com o uso de TDES ou AES para proteger o PIN. Além disso, se o PIN precisar ser protegido durante o transporte em POIs offline não integrados, o POI deverá ser compatível com o uso de TDES ou AES para esse canal. "Offline" significa que o POI é compatível com a verificação de PIN offline pelo chip integrado do cartão de pagamento. A menos que indicado de outra forma, a designação "Offline", sem qualquer sufixo, na *Lista de aprovação de dispositivos de PTS da PCI* representa que o POI oferece recursos de verificação de PIN offline em texto simples e cifrado. A designação "Offline (p)" com o "(p)" como sufixo representa que o POI offline conta com recursos somente para verificação de PIN offline de texto simples. ***Observação:*** *Todos os POI de verificação de PIN offline recém-aprovados devem ter recursos de verificação de PIN em texto simples e cifrado.* No entanto, sob os testes atuais, todos os dispositivos de POI off-line recém-avaliados devem ter recursos de verificação de PIN em texto simples e cifrado. Os SCRs ou outros dispositivos de POI que incluem um ICCR ou um leitor híbrido devem ter uma designação "offline" para serem usados para aceitação de PIN offline.

Recurso e aplicabilidade	Descrição
Gestão de criptografia de chave de PIN (PED, EPP, SCRP, UPT)	**"Gerenciamento de chaves de criptografia de PIN"** indica se o laboratório avaliou com sucesso o dispositivo de segurança de pagamento para permitir o uso de DES Triplo (TDES) ou AES para criptografia de PIN para PIN online. O TDES exige o uso de pelo menos uma chave de comprimento duplo. Uma MK/SK (chave mestra, chave de sessão), DUKPT e/ou designação fixa indicam que o dispositivo foi avaliado com sucesso para apoiar a implementação do TDES para esses esquemas específicos de gerenciamento de chaves. ***Observação:*** *A DUKPT é o único algoritmo (UKPT) de transação por chave (ANSI X9.24) que a PCI reconhece e aprova; todas as outras formas de UKPT testadas pelo laboratório não serão descritas na carta de aprovação ou no site da PCI PTS.* Quando o AES for utilizado, isso será explicitamente informado em conjunto com as metodologias MK/SK, DUKPT ou de chave fixa. Isto é para dispositivos de POI sem recursos para a entrada de PINs online e, em geral, isso será N/A para dispositivos nas classes de aprovação não-PED ou SCR e, por definição, será N/A para dispositivos PIN offline somente. ***Observação:*** *os dispositivos de POI v5 e v6 usados para PIN online devem ser compatíveis com o formato de bloco de PIN ISO 4 (AES).*
Gerenciamento de Chaves SRED (PED, EPP, SCR, SCRP, UPT)	**"Gerenciamento de chave SRED"** indica se o laboratório avaliou com sucesso o dispositivo de segurança de pagamento para apoiar o uso de DES Triplo (TDES) ou AES na criptografia de dados de conta. O TDES exige o uso de pelo menos uma chave com comprimento triplo ou DUKPT para criptografia de dados de conta. Uma MK/SK (chave mestra, chave de sessão), DUKPT e/ou Designação fixa indicam que o dispositivo foi avaliado com sucesso para apoiar a implementação do TDES para esse(s) esquema(s) específico(s) de gerenciamento de chaves. Onde AES for utilizada, será explicitamente observado em conjunto com as metodologias MK/SK, DUKPT ou Chave Fixa. A criptografia de preservação do formato (FPE) deve ser indicada quando um dos algoritmos aprovados ANSI, ISO ou NIST for utilizado. ***Observação:*** *aplica-se somente aos dispositivos de POI v6.*

Recurso e aplicabilidade	Descrição
Controle de aviso (PED, EPP, UPT)	▪ **Controlada pelo fornecedor:** o usuário final, o adquirente ou o revendedor não pode modificar o firmware ou o aplicativo de pagamento POS POI atendido para fazer alterações nos prompts do dispositivo ou nos controles de entrada de PIN. Somente o fabricante do equipamento original do POI é capaz de modificar as instruções e os controles para a entrada do PIN. ▪ **Controlado pela instituição compradora:** o fabricante do equipamento original enviou o POI POS atendido com mecanismos para controlar a tela POI e seu uso no local. Esses mecanismos podem ser empregados para desbloquear o POI para atualizações dos prompts pelo adquirente, usando processos adequados e controlados por criptografia, conforme definido no requisito de segurança POI aplicável. O revendedor ou usuário final, se autorizado pelo adquirente, também pode fazer atualizações com processos controlados e criptograficamente adequados. Não aplicável a dispositivos sem tela. Os dispositivos devem ser implantados bloqueados. De qualquer forma, o cliente adquirente será **sempre** responsável por garantir que processos apropriados e procedimentos documentados estejam em vigor para controlar a exibição e o uso do POI.
Tecnologia de Entrada de PIN (PED, EPP, UPT)	**"Tecnologia de entrada de PIN"** indica qual tecnologia é implementada para capturar o PIN de titulares do cartões. O valor para este campo pode ser: ▪ **Teclado físico:** conjunto de botões organizados em um bloco que tem dígitos e opcionalmente letras, em conformidade com a norma ISO 9564. ▪ **Tela de toque:** tela que pode detectar a presença e a localização de um toque dentro da área de exibição e permitir que o titular do cartão digite o PIN. ▪ **N/A:** para HSMs, não PEDs, e para SCRs e SCRPs exceto conforme indicado na classe de aprovação SCR ou SCRP. Um dispositivo não pode ser compatível com uma versão do teclado físico e uma versão de tela de toque sob a mesma aprovação, onde ambos podem ser usados para entrada de PIN. Pode dar suporte a um dispositivo que tenha ambas as interfaces relacionadas com o fornecimento de suporte às leis nacionais ou locais de deficiência.

Recurso e aplicabilidade	Descrição
Componentes Aprovados (PED, UPT)	**"Componentes aprovados"** contêm, quando relevante, a lista de subcomponentes aprovados que fazem parte do dispositivo aprovado e que passaram por uma avaliação distinta com sucesso. Cada componente é listado com seu número de aprovação. O uso de um dispositivo com componentes (por exemplo, EPPs, leitores de cartões) diferentes dos listados como um componente aprovado para esse dispositivo invalida a aprovação desse dispositivo.
Funções Fornecidas (PED, EPP, UPT, SCR, SCRP, não-PED)	"**Funções fornecidas**" indica quais das funções a seguir são compatíveis com o dispositivo. Uma ou mais das opções a seguir podem ser aplicadas, dependendo da implementação: ▪ **Entrada de PIN:** o dispositivo permite a captura de PIN de titulares de cartões. ▪ **Recursos do leitor de cartão:** o dispositivo possui componentes que podem capturar dados de cartão, como leitor de tarja magnética (MSR) ou leitor ICC (ICCR) ou sem contato (CTLS). ***Observação:*** *os leitores sem contato somente são considerados compatíveis com o uso do P2PE se a Classe de aprovação em questão tiver sido validada para o SRED. Além disso, algumas aprovações de dispositivos podem ter versões validadas para SRED e outras não. Se tal mistura ocorrer, somente os dispositivos que utilizarem uma versão de firmware designada para SRED serão validados para atender aos requisitos de segurança do leitor sem contato. Nos dispositivos com leitores sem contato usando firmware que não forem validados para o SRED, os leitores sem contato não serão validados para quaisquer requisitos de segurança.* ▪ **Tela:** o dispositivo tem uma tela integrada usada para avisos ao titular do cartão e, possivelmente, a apresentação de outras informações. ▪ **SRED:** o dispositivo atendeu aos requisitos aplicáveis de leitura e intercâmbio seguros de dados ▪ **OP:** o dispositivo atendeu aos requisitos aplicáveis dos protocolos abertos.

Recurso e aplicabilidade	Descrição
Outras informações	Este campo pode ser utilizado para inserir qualquer informação adicional pertinente. Por exemplo, se um fornecedor tiver alterado o status de um dispositivo para fim da vida útil (EOL), conforme descrito em 5.4, “Taxa de Listagem de Aprovação” e, portanto, o dispositivo não estiver mais disponível para compra, exceto para fins de manutenção sujeitos às regras da bandeira de pagamento. Dispositivos com status EOL não são mais suportados pelo fornecedor e nenhum deltas é processado para esses dispositivos. A data e o mês de EOL serão listados no site. Utilizado também para HSMs v2 e v3 para delinear se eles são aprovados para uso restrito ou irrestrito, conforme delineado nos Requisitos de Segurança de HSM: ▪ **Restrita —** A aprovação é válida somente quando implantada em ambientes controlados ou mais robustos (por exemplo, Ambientes Seguros) conforme definido na ISO 13491-2 e na Política de Segurança HSM da PCI do dispositivo. ▪ **Irrestrita —** A aprovação é válida em qualquer ambiente. Os dispositivos compatíveis com o formato de bloco de PIN ISO 4 (AES) serão indicados aqui. Para mais informações sobre se há compatibilidade com as metodologias MK/SK, DUKPT ou de chave fixa pelos blocos de PIN AES, consulte a seção de gerenciamento de chaves.
Formato do dispositivo	Todos os componentes relevantes para a segurança (PIN pad, tela, leitor(es) de cartão) do dispositivo são mostrados em uma ou mais imagens. Ao menos uma das imagens deve atender ao requisito de que o número da versão do hardware deve ser mostrado em uma etiqueta anexada ao dispositivo. Note que, para dispositivos com várias versões de hardware aprovadas, somente uma dessas ilustrações é necessária para facilitar aos compradores desses dispositivos o reconhecimento de como determinar as versões aprovadas.

Apêndice B: Avaliações Delta — Guia de Escopo

B.1 Introdução

O PCI SSC reconhece que os fornecedores podem precisar fazer correções de manutenção em dispositivos validados da PTS que o fornecedor já vendeu, mas ainda dá suporte. Em adição, os fornecedores podem optar por portar versões atualizadas do firmware que foram aprovadas em relação aos requisitos de segurança mais recentes para produtos para os quais a aprovação expirou. Isso pode acontecer porque os clientes de um fornecedor desejam padronizar sua implantação em relação a uma determinada versão do firmware e/ou adicionar funcionalidade a esse dispositivo.

Este apêndice fornece diretrizes sobre se as mudanças feitas pelos fornecedores em um dispositivo PTS validado (se POI ou HSM) são limitadas o suficiente no escopo, de modo que seja permitido que essas alterações no dispositivo PTS validado possam ser avaliadas como um "delta" para a validação original. Qualquer alteração de hardware em um dispositivo aprovado que tenha sido implantado deve resultar em uma nova versão de n.º de hardware Qualquer alteração de firmware em um dispositivo aprovado deve resultar em uma nova versão de firmware. Os dispositivos devem passar por uma avaliação delta quando tais alterações forem feitas.

B.2 O que é uma avaliação Delta?

Todas as avaliações iniciais sob uma versão principal (por exemplo, 1.x, 2.x, 3.x. 4.x, 5.x, 6.x etc.) dos requisitos de segurança de um certo produto constituirão uma nova avaliação e devem receber um novo número de aprovação.

As revisões dos dispositivos que foram aprovados são denominadas "deltas". As revisões Delta envolvem o Laboratório Reconhecido PTS (ou "Laboratório PTS") avaliando as alterações com base na versão principal mais atual dos requisitos de segurança usados para a avaliação original e a publicação mais atual de perguntas frequentes associadas a esses requisitos. Por exemplo, caso um dispositivo tenha sido originalmente avaliado contra o PTS POI v6.0, qualquer avaliação delta teria que ser realizada com v6.1 (a versão mais atual do PTS v6.x e as últimas perguntas frequentes v6.x emitidas). Exemplos de deltas:

- Revisões para firmware ou hardware existentes em dispositivos já aprovados para adicionar ou modificar a funcionalidade.
- Adicionando EMV Nível 1 em uma aprovação existente.
- Correções da manutenção em dispositivos que tenham aprovações expiradas.
- Avaliação de um dispositivo para entrada de PIN offline onde a aprovação existente é apenas para entrada de PIN online, ou vice-versa.
- A portabilidade de um conjunto novo de firmware para um dispositivo aprovado existente.

As avaliações delta não podem levar um produto previamente aprovado sob um número de versão principal anterior do padrão PTS POI, como 5.x, para uma aprovação sob outro número de versão principal, como 6.x.

As Dúvidas frequentes só precisam ser aplicadas a qualquer aspecto do dispositivo que for afetado pelas alterações feitas pelo fornecedor. Por exemplo, se um fornecedor fizesse alterações no layout de hardware do projeto POI, mas não alterasse o firmware de forma alguma, todas as entradas de FAQ atualizadas que afetassem somente o firmware não seriam aplicadas à avaliação delta. Isso está explicado com mais detalhes na seção "Processo de avaliação detalhada" do *Guia de teste e aprovação de dispositivos PCI PTS.*

B.3 Como determinar se um Delta é permissível

O potencial das mudanças e seus impactos não podem ser identificados antecipadamente. As alterações devem ser avaliadas individualmente. Os fornecedores devem entrar em contato com um dos Laboratórios PTS para receberem orientação. Os Laboratórios PTS devem consultar a PCI conforme necessário antes de enviar um relatório delta para determinar se um conjunto de mudanças é bom demais para ser abordado no processo delta. Os laboratórios determinarão se a mudança afeta a segurança. Em todos os casos, as alterações que afetam a segurança exigem uma avaliação que deve ser apresentada no relatório delta. No mínimo, para um determinado tipo de mudança, todos os requisitos identificados nos quadros abaixo devem ser avaliados quanto ao impacto na segurança. Deve ser apresentada uma justificativa no relatório delta para cada mudança que estiver determinada como não tendo afetado a segurança.

B.3.1 Impactos de certas mudanças na amostra

As subseções a seguir relacionam uma lista não exaustiva de alterações de exemplo que, tomadas individualmente, são permitidas para consideração por meio do processo delta. A inclusão de muitas dessas alterações, especialmente quando se considera uma série de mudanças no hardware do dispositivo, deve ser considerada como um novo dispositivo que requer uma avaliação completa para a versão mais recente do padrão PTS atual.

B.3.2 Mudanças de firmware

De modo geral, todas e quaisquer alterações feitas no firmware executado em um dispositivo PTS previamente aprovado podem ser consideradas em uma única avaliação delta, exceto quando a alteração é vista como muito difundida, como uma alteração no SO, como mudança de um sistema proprietário para um sistema baseado em aberto. A seguinte tabela identifica diversos tipos de alterações de firmware e os requisitos da PTS que, no mínimo, devem ser considerados ao avaliar cada tipo de alteração. Os Laboratórios de PTS que avaliam tais mudanças podem justificar a exclusão de qualquer requisito identificado ou a inclusão de requisitos adicionais com base em sua avaliação das alterações.

Tabela 8: Tipos de mudanças de firmware e Requisitos impactados

As alterações aceitáveis de firmware que podem ser consideradas em uma avaliação delta são, entre outras:

Tipo de alteração de firmware	Requisitos impactados					
	Versão padrão de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Qualquer mudança de hardware	N/A	N/A	N/A	B20	B20	B20
Mudanças de firmware sem impacto aparente nos Requisitos da PCI	B3	B3	B3, F1, G1, H1, I1	B3, F1	B3, F1	D2, E2
Alterações na metodologia de recuperação de violação segura	B1	B1	B1	B1	B1	B1
Tratamento de erros (ou seja, transbordamento de dados)	A5, B2	A3, B2	A3, B2	A3, B2	A2, B2	A3, D1
Alterações aos protocolos de comunicações externas	B2	B2	B2, F1, G1, H1, I1	B2, F1	B2, F1	D1, D2
Alterar aos mecanismos de atualização de software/firmware	B3, B4	B3, B4	B3, B4, J4	B3, B4, B4.1, J4	B3, B4, B4.1, J4	E2, B2, B2.1,
Novo esquema para autenticação de firmware/aplicativo	B4	B4	B4	B4, B4.1	B4, B4.1	B2, B2.1
Alterações aos tempos limite de dígitos de PIN	B7, C3	B6, B10	B6, B10	B6, B10	B6, B10	B4, B8
Alterações das funções criptográficas	B10, C2, C4, C6, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B4, B7, B11, B12, B21
Alterações não relativas à segurança do firmware do leitor de cartões	D4	A11, D4	A10, D4	A9, D4	A8, D4	A10, B21
Alterações a mecanismos de autenticação de serviço confidenciais	B8, B9	B7, B8	B7, B8	B7, B8	B7, B8	B5, B6
Atualização da metodologia de carregamento de chave	C5	B11	B11, J4	B11, J4	B11, J4	B9, B2

Tipo de alteração de firmware	Requisitos impactados					
	Versão padrão de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Alterações da gestão de chaves	C1, C5, C6, C7, C8	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B9, B12, B13, B18, A13
Alteração para hierarquia de chaves	C1, C5, C7	B11, C1, D1	B11, C1, D1	B11, C1, D1	B11, C1, D1	B9, B18, A13
Alterações do armazenamento de chaves	C1, C5	B11, D1	B11, D1	B11, D1	B11, D1	B9, A13
Tipos novos de chaves	C1, C5, C6	B11, B13, D1	B11, B13, D1	B11, B13 D1	B11, B13 D1	B9, B12, A13
Alterações no tratamento do comprimento dos PIN	C4, D4	B12, D4	B12, D4	B12, D4	B12, D4	B11, B21
Pequenas mudanças na interface do usuário	B5, B6	B5, B15	B5, B15, F1 G1, H1, I1	B5, B15, F1	B5, B15, F1	B3, B14, D2
Avisos atualizados de PIN	A7, B5, B6	A8, B5, B15	B5, B15, B16	B5, B15, B16	B5, B15, B16	B3, B14, B15
Inclusão de funcionalidade SRED ***Observação:*** *deltas SRED em dispositivos v2.x não serão aceitos após 31 de dezembro de 2012.*	N/A	N/A	B17-19, K1-25	B17-19, K1-23	B17-19, K1-23	B1, B2, B2.1, B2.2, B4, B5, B6, B7, B9, B10, B12, B16, B16.1, B16.2, B17, B19, B22–B26, A2, A4, A6, A7, A10-A14, D1

B.3.3 Mudanças de firmware

As mudanças feitas pelos fornecedores no hardware de dispositivos PTS previamente aprovados só são permitidas se o escopo de tais alterações for limitado.laboratórios de PTS A seguinte tabela identifica diferentes tipos de alterações de hardware e os requisitos da PTS que, no mínimo, devem ser considerados ao avaliar cada tipo de alteração. Os laboratórios de PTS que avaliam tais mudanças podem justificar a exclusão de qualquer requisito identificado ou a inclusão de requisitos adicionais com base em sua avaliação das alterações.

A inclusão de mais que quatro (4) dos tipos de alteração de hardware identificados, tal como delineados na tabela abaixo numa única apresentação delta de um dispositivo de PTS previamente aprovado pode representar efetivamente um novo dispositivo que deve ser submetido à sua própria avaliação completa, em relação à versão mais recente do Padrão PTS atual. Os candidatos a envios delta que ultrapassarem esse limite que, na opinião do Laboratório PTS, representarem uma pequena alteração no dispositivo de PTS aprovado, devem ser apresentados ao PCI SSC antes de completar a avaliação para determinar se o escopo de mudança é muito grande. Tampouco é aceitável apresentar uma série de envios delta com alterações de hardware como tentativa de contornar esse limite. Se forem recebidos envios delta com mudanças de hardware dentro de três meses após a aprovação do dispositivo de referência, deverá haver informações suficientes acompanhando o envio para justificar a necessidade da alteração e e a não inclusão como parte do envio previamente aprovado. Em todos os casos, as mudanças cumulativas serão consideradas na avaliação da propriedade de qualquer solicitação delta específica.

Por exemplo, um fornecedor faz uma mudança nas grades de adulteração e no roteamento de sinal em seis PCBs dentro de um dispositivo. De acordo com o direcionamento de escopo delta, a inclusão de quatro ou mais tipos de alteração de hardware em uma única submissão delta para um dispositivo de PTS previamente aprovado pode efetivamente representar um novo dispositivo que deve estar sujeito a sua própria avaliação completa em relação à versão mais recente do padrão PTS atual. Neste exemplo, isso não conta como seis alterações, mas como uma única mudança, uma vez que são todas da mesma mudança “tipo”. Isso atende os critérios de um delta.

Um dispositivo enviado com alterações internas de hardware suficientes para exigir uma nova avaliação—, mas sem alterações externas—não pode ser enviado como um delta, mesmo que a aparência externa seja idêntico. O grau de alterações feitas internamente exige que o dispositivo receba uma avaliação completa em relação à versão de requisitos atualmente disponíveis para uso em novas avaliações. Se a avaliação for bem-sucedida, isso resultará em um novo número de aprovação. Além disso, enquanto o novo dispositivo terá uma versão de hardware diferente do dispositivo existente, também é necessário ter um novo nome/número de modelo. O objetivo é evitar confusão no mercado, especialmente se surgirem problemas após a implantação impactando apenas uma das aprovações, mas não a outra(s).

Substituir um PCB não conta como uma mudança única. Todas as alterações relacionadas à mudança PCB precisam ser levadas em consideração. Por exemplo, mudar o PCB re-direciona a grade de adulteração e sinais. Isso iria contar como um. A movimentação de um processador também iria contar como uma mudança e precisa ser avaliada em conformidade. Quaisquer outras mudanças relevantes na segurança resultantes da mudança no PCB também aumentariam para a contagem de alterações.

Qualquer alteração no hardware de um PED aprovado, mesmo para os componentes não relacionados à segurança, pode afetar direta ou indiretamente a segurança do dispositivo. Assim sendo, qualquer avaliação delta que incluir modificações no hardware do dispositivo aprovado, mesmo os circuitos não relacionados às funções de segurança do dispositivo, deverá, no mínimo, ser revisada pelo laboratório PTS em relação ao impacto potencial nos seguintes requisitos de segurança da versão aplicável da Norma PTS contra a qual a avaliação sendo realizada:

- V1.x: Requisitos A1, A2, A3 e C1
- V2.x: Requisitos A1 e A7
- V3.x: Requisitos A1 e A7
- V4x: Requisitos A1, A6, B2 e B20
- V5x: Requisitos A1, A5, B2 e B20
- V6x: Requisitos A1, A5, B2 e B20

Tabela 9: Mudanças de hardware aceitáveis

Alterações aceitáveis de hardware que podem ser consideradas em uma avaliação delta incluem, mas não se limitam a:

Tipo de alteração de hardware	Requisitos afetados					
	Versão do padrão de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Qualquer mudança de hardware[2]	A1, A2, A3, C1	A1, A7	A1, A7	A1, A6, B2, B20	A1, A5, B2, B20	A1, A2, A6, D1, B20
Alterações nos plásticos de revestimento (por exemplo, dimensões de abertura da tampa, áreas que permitem o acesso interno,) ou telas somente de saída. Os dispositivos alterados devem continuar consistentes com o formato original e as características visíveis do dispositivo.[3]	A4, A7, A9–A11, D1–D4	A2, A6, A8–A11, D1–D4	A2, A6, A8–A11, B16, D1–D4, K1–K3	A5, A7–A9, A11, B16, D1–D4 K1–K3	A4, A6–A8, A10, B16, D1–D4 K1–K3	A5, A7-A9, B5, B15, B21, A13, A14, A11, A12, A6
Modificação em chaves de adulteração/remoção (por exemplo, alterações nos materiais, desempenho, localização, circuitos, resposta de adulteração, etc.) ou recursos de resistência contra/apresentação de sinais de violação	A5, D1	A2, A3, A11, D1	A2, A3, A10, D1	A2, A9, D1	A2, A8, D1	A3, A10, A13
Modificações ou substituição de qualquer processador usado pelo dispositivo [4]	A5, A6, A7, A9, B1-B10, C2-C8, D4	A3, A4, A6, A8, B1-B15, C1, D4	A3, A4, A6, A8, A11, B1-B19, C1, D4	A3, A4, A5, A7, A10, B2–B19, C1, D4	A2, A3, A4, A6, A9, B2–B19, C1, D4	A3, A4, A5, A6, A7, B2-B19, B21

[2] Este item não deve ser incluído na contagem de alterações ao determinar se o número de alterações em um único envio delta está no intervalo aceitável de quatro (4). Todas as alterações de hardware exigem uma alteração no número da versão do hardware feita de acordo com o Apêndice A.

[3]" Características visíveis" referem-se à aparência e ao funcionamento do dispositivo, inclusive suas dimensões físicas. "Dimensões físicas" referem-se ao tamanho físico do dispositivo, medido sobre as partes superior e inferior ou, no caso de um dispositivo circular, sua circunferência. A espessura ou a profundidade do dispositivo também é considerada em suas dimensões físicas. Por exemplo, a inclusão ou remoção de impressora, tela LCD, leitor de código de barras ou compartimento de bateria estendido que altere a profundidade do dispositivo é aceitável, desde que não altere a segurança do dispositivo. As alterações a serem permitidas como delta não devem ser superiores a 10% da dimensão linear mais longa do dispositivo. Por exemplo, um dispositivo com 10 polegadas de comprimento pode ser alterado a até pelo menos 9 polegadas ou não mais do que 11 polegadas de comprimento como parte de um delta. No entanto, mesmo como um delta, ele exigirá uma alteração de nome de modelo que pode ser relacionada em conjunto com a listagem original.

[4] Cada modificação ou substituição do processador conta como uma alteração de hardware separada (por exemplo, se o processador seguro e o processador de aplicativos fossem modificados, isso contaria como duas alterações de hardware)..

Tipo de alteração de hardware	Requisitos afetados					
	Versão do padrão de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Alterações nas interfaces de usuário que podem ser utilizadas para entrada de PIN (por exemplo, telas sensíveis ao toque, membranas do teclado, botões, etc., mas excluindo modificações das teclas de função)	A5, A7, A9, D1	A2, A6, A8, A9, A11, D1	A2, A6, A8-A10, B16, D1	A5, A7-A9, A11, B16, D1	A4, A6-A8, A10, B16, D1	A5, A8-A10, B5, B15, A13
Substituição ou inclusão de qualquer leitor [5]	D1-4	A10, A11, D1-4	A10, D1-D4, K1, K2	A9, D1-D4 K1-K2	A8, D1-D4 K1-K2	A10, A11-A14, B21
Modificações nos circuitos de comunicação	A5, B2, D1	A2, A3, B2, D1	A2, A3, B2, D1, F1, G1, H1, I1	A3, B2, D1, F1	A2, B2, D1, F1	A3, A13, D1, D2
Modificações nos circuitos de potência	A5	A3	A3	A3	A2	A3
Modificações em outros componentes principais do circuito PCB (por exemplo, circuitos de áudio, circuitos de aquecimento, etc.). [6,7]	A5, A8	A3, A5	A3, A5	A3, A11	A2, A10	A3, B5

B.4 Como envolver um Laboratório da PTS para realizar uma avaliação Delta

Os fornecedores podem selecionar um Laboratório PTS diferente para proceder com uma avaliação delta além do Laboratório PTS usado para realizar a avaliação inicial ou avaliação delta anterior. Contudo, o Laboratório PTS subsequente (“Laboratório Delta”) é livre para determinar o nível de confiança que deseja colocar no trabalho anterior do Laboratório PTS e será responsável por quaisquer reivindicações de conformidade geradas por meio da revisão delta; e isso pode resultar em trabalho além do que seria necessário de outra forma. Para os relatórios da versão 3 ou superior, o Laboratório Delta terá acesso ao(s) relatório(s) anterior(es) do Laboratório PTS, incluindo todos os relatórios de componentes delta ou OEM subsequentes à avaliação original. Se esses relatórios não estiverem disponíveis, o Laboratório Delta recusará o contrato ou então deverá concluir uma avaliação completa do dispositivo.

[5] Cada alteração do leitor conta como uma mudança de hardware separada. Por exemplo, se o MSR e o ICCR forem alterados, contará como duas alterações de hardware separadas. No entanto, uma alteração envolvendo um leitor híbrido conta como apenas uma mudança de hardware.

[6] Isso exclui o redirecionamento de circuitos.

[7] A substituição completa ou o redesenho de uma PCB que adicione ou remova funcionalidades ou recursos de segurança requer uma avaliação completa.

B.5 Requisitos de documentações Delta

B.5.1 Orientação de relatórios para fornecedores de PTS

Todas as mudanças feitas nos dispositivos aprovados pela PTS devem ser divulgadas pelo fornecedor PTS. Recomenda-se que os fornecedores de PTS enviem um documento da análise de alterações ao laboratório de PTS contendo as seguintes informações, no mínimo:

- Nome do dispositivo de PTS aprovado;
- Números novos de hardware, firmware e versão do aplicativo, conforme aplicável, a serem avaliados;
- Detalhes do dispositivo de PTS aprovado atualmente na lista de dispositivos PTS aprovados que estiverem sendo utilizados como referência para a avaliação;
- Informações do laboratório de PTS que executou a avaliação original no dispositivo e informações sobre quaisquer avaliações delta subsequentes feitas nesse dispositivo desde a aprovação original;
- Descrição da alteração;
- Descrição de por que a alteração é necessária;
- Descrição de como a alteração funciona;
- Explicação de como e por que os requisitos de PTS são afetados;
- Descrição dos testes realizados pelo fornecedor para validar como os requisitos de segurança de PTS são afetados; e
- Descrição de como a identificação (versionamento) da alteração se encaixa na metodologia de controle de configuração do fornecedor.

B.5.2 Requisitos de comunicação para laboratórios de PTS

Os relatórios de avaliação delta devem apresentar todas as informações relevantes sobre as alterações e as avaliações das alterações, equivalentes aos níveis de pormenor especificados nas DTRs. Os laboratórios de PTS devem fornecer a seguinte documentação com cada envio delta:

- O número de todos os tipos de mudanças de hardware identificadas;
- Uma descrição de alto nível que defina claramente todas as mudanças feitas no dispositivo de PTS aprovado;
- Citações de:
  - O relatório de aprovação de referência e quaisquer envios delta subsequentes em que a apresentação atual delta se baseia, e
  - Toda a documentação de apoio utilizada para fundamentar as conclusões representadas na apresentação delta;
- Uma tabela que apresenta as seguintes informações, sobre cada alteração, incorporada na atualização do dispositivo de PTS aprovado a partir da configuração previamente aprovada:
  - Uma descrição da alteração;
  - Identificação do item ou dos itens de configuração alterados (arquivos de sistema ou componentes de hardware) afetados pela alteração;
  - Uma avaliação de alto nível do impacto da mudança em segurança;

- Identificação dos Requisitos de Segurança PTS que são afetados pela alteração (incluindo requisitos para os quais as respostas anteriores permanecem precisas sem alteração); e
- Uma descrição de alto nível dos testes concluídos, se houver, utilizada na validação da avaliação;

- Respostas atualizadas pelos requisitos de segurança de PTS afetados que descrevem claramente as alterações necessárias às avaliações de referência.

B.6 Aplicabilidade de dúvidas frequentes durante avaliações Delta

As dúvidas técnicas frequentes são atualizadas regularmente para não apenas acrescentar esclarecimentos aos requisitos, para proporcionar condições de concorrência consistentes e equitativas nos aplicativos desses requisitos, mas também podem abordar novas ameaças à segurança que surgiram. Como tal, As Dúvidas técnicas frequentes estão geralmente em vigor imediatamente após a publicação.

O objetivo não é fazer com que um dispositivo em avaliação falhe devido à publicação de Dúvidas frequentes após a aprovação desse dispositivo. Contudo isso pode ser necessário se existirem explorações conhecidas que alterem significativamente o ambiente de ameaça para o dispositivo a partir de quando ele foi avaliado originalmente. A menos que haja uma ou mais dessas façanhas, um produto atualmente em avaliação geralmente não estará sujeito a novas dúvidas frequentes emitidas durante a avaliação do produto. Isto não isenta um produto da aplicabilidade das dúvidas frequentes se o produto tiver que ser reformulado e reenviado posteriormente devido a outros problemas que levem à sua falha na avaliação.

Os dispositivos que passam por avaliações delta devem levar em conta as perguntas frequentes atuais da versão principal associada dos requisitos de segurança, somente para os requisitos de segurança afetados pela alteração delta. Por exemplo, se uma alteração afetar a conformidade dos Requisitos B1 e B4, somente as dúvidas frequentes atuais associadas a B1 e B4 deverão ser levadas em consideração como parte do delta.

Além disso, não basta para o laboratório determinar que a mudança não diminui a segurança do dispositivo. Devido à evolução das ameaças e às técnicas de ataque a partir do momento da avaliação original (que pode ter ocorrido muitos anos antes), o laboratório deve determinar que o dispositivo ainda atende aos requisitos de segurança relevantes afetados pela mudança, dadas as mudanças nos vetores de ataque. Isso ocorre porque, se os deltas forem feitos para melhorar ou corrigir a funcionalidade ou para outros fins, o resultado final é para prolongar a vida útil do dispositivo no mercado.

Em todos os casos, o Laboratório PTS que executa a avaliação deverá aconselhar o PCI SSC sobre as circunstâncias, e o PCI SSC tomará a decisão final com base nas circunstâncias. Além disso, tanto para avaliações novas como as delta, o Laboratório de PTS também indicará em seu envio a versão dos requisitos de segurança utilizados nas avaliações, bem como a data de publicação das FAQs técnicas utilizadas.

B.7 Considerações para componentes atualizados em terminais integrados

Os fornecedores com dispositivos de PTS aprovados que integrarem outros componentes de PTS aprovados pela OEM (tal como terminais de pagamento autônomos) podem procurar por avaliações delta em tais dispositivos por alterações que ocorrem nos componentes OEM incorporados, inclusive a substituição de qualquer componente OEM por um modo diferente (por exemplo, um ICCR OEM aprovado em separado, produzido por um fornecedor será substituído no formato final do terminal integrado ou UPT por outro modelo, até mesmo de outro fornecedor). Este subsídio é aplicado desde que o fornecedor continue a ter controle sobre a montagem e a fabricação final do terminal integrado ou UPT.

As alterações que ocorrem no próprio formato final (por exemplo, caixa), devido à complexidade da integração, devem passar por testes como uma nova avaliação contra uma versão de requisitos que não tenha sido retirada do uso para novas avaliações.

Contudo, em todos os casos, todos os requisitos de segurança afetados serão avaliados, inclusive os não aplicáveis anteriormente (por exemplo, se o novo invólucro introduzir dispositivos adicionais de interface de titulares do cartões não presentes na avaliação original).

Apêndice C: Solicitação de alteração administrativa de PTS

Mudanças administrativas que afetam um dispositivo de PTS aprovado, o nome comercial e/ou o endereço do fornecedor de PTS ou os detalhes de contato devem ser divulgados neste documento de *Alteração administrativa*. Os fornecedores devem preencher todas as seções e, em seguida, enviar o documento para um laboratório reconhecido pela PCI. O laboratório deve então enviar a documentação de suporte necessária por meio de uma alteração administrativa para o PCI SSC para revisão. As alterações que contiverem novas imagens devem ter as imagens enviadas por meio de um envio delta.

Detalhes da empresa fornecedora PTS			
Nome da empresa		Data de envio	
Nome da pessoa que solicita a alteração		Endereço de e-mail:	
Cargo da pessoa que solicita a alteração		Função (primária, faturamento, técnico)	

Descrição da(s) mudança(s)				
Tipo de mudança (marque todas as opções válidas)	☐ Nome comercial	☐ Endereço comercial	☐ Nome(s) do modelo do dispositivo	☐ Nome/endereço de contato
Descreva brevemente o motivo das mudanças				

Informações atualizadas da empresa			
Novo nome comercial		Novo site	
Endereço postal			
Endereço de cobrança			

Modelo(s) do dispositivo			
Número de aprovação de PTS	**Nome do modelo**	**Novos detalhes do modelo**	
		Novo nome do modelo	Imagem incluída *
			☐
			☐
			☐
			☐
			☐
			☐

Modelo(s) do dispositivo			
Número de aprovação de PTS	**Nome do modelo**	**Novos detalhes do modelo**	
		Novo nome do modelo	Imagem incluída *
			☐
			☐
			☐
			☐

** Em "Novas imagens do modelo do dispositivo" na última página.*

Contato principal/comercial			
Nome do contato		Cargo comercial	
E-mail de contato		Telefone de contato	

Contato de faturamento *(as faturas serão enviadas para este endereço individual/e-mail)*			
Nome do contato		Cargo comercial	
E-mail de contato		Telefone de contato	

Contato técnico			
Nome do contato		Cargo comercial	
E-mail de contato		Telefone de contato	

Documentação de apoio necessária

	Mudança administrativa (este formulário)	Política de segurança	Contrato de liberação do fornecedor (VRA)	Imagens do dispositivo*
Mudança de mome comercial	**X**	**X**	**X**	**X**
Nome do modelo do dispositivo	**X**	**X**		**X**
Nome do contato principal	**X**			

** Se as imagens aplicáveis precisarem ser enviadas por meio de um envio delta.*

Apêndice D: Atestado de validação de PTS

Instruções de envio

O fornecedor de PTS deve preencher este documento como uma declaração do status de validação do firmware com os requisitos de segurança PTS POI ou HSM, conforme aplicável. Os fornecedores ou outros terceiros que forem licenciar produtos aprovados de outros fornecedores para comercializar ou distribuir sob seus próprios nomes não são obrigados a preencher esta declaração se as licenças não implicarem em nenhuma alteração no firmware, exceto se houver atualizações baseadas nas mesmas alterações que o fornecedor OEM fez no seu próprio produto no qual se baseia o produto licenciado.

O fornecedor de PTS deve preencher todas as seções aplicáveis e enviar este documento junto com cópias de toda a documentação de validação necessária para PCIPTS@pcisecuritystandards.org de acordo com as instruções do PCI SSC para envio de relatórios, conforme descrito no *Guia do programa de estes e aprovação de dispositivos de PTS* .

Parte 1. Fornecedor de PTS					
Nome da empresa:					
Nome do contato:			Título:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		Código postal:	
URL:					

Parte 2. Informações de aprovação do dispositivo

Para cada aprovação de HSM ou POI não expirada a partir do ano anterior que terminar em 31 de dezembro, indique o status de envio do firmware como:

A: Nenhuma modificação foi feita na versão do firmware.

B: Todas as mudanças de hardware e firmware foram avaliadas por um laboratório de PTS em um relatório apresentado à PCI, incluindo as versões de hardware ou firmware identificadas que utilizam uma metodologia validada de versão variada (curinga). No caso dos dispositivos de POI, isso inclui todas as vulnerabilidades identificadas pelo fornecedor em cada um dos protocolos e interfaces definidos no requisito de segurança POI D1, conforme evidenciado pelo processo de avaliação de vulnerabilidade enumerado sob E10 a E12 dos DTRs da POI.

Para todos os dispositivos não compatíveis com protocolos abertos, o fornecedor deve apresentar provas de que há um registro auditável de um processo de avaliação de vulnerabilidade contínuo fornecendo uma cópia do formulário de aprovação do fornecedor especificado no requisito de POI E10 para o ano anterior que termina em 31 de dezembro.

Número de aprovação de PTS	Data de expiração da aprovação	Nome do modelo	Versão do firmware	Status do envio do firmware para os 12 meses que terminam em 31 de dezembro do ano anterior	
				A	B
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐

Parte 3. Reconhecimento do fornecedor de PTS	
Assinatura do diretor executivo do fornecedor PTS ↑	*Data ↑*
Nome do diretor executivo do fornecedor PTS ↑	*Título ↑*
Empresa fornecedora PTS representada ↑	

Apêndice E: Atestado de dispositivos de PTS

O fornecedor de PTS deve preencher este documento como uma declaração do status de validação do dispositivo com os requisitos de segurança de PTS da POI. O fornecedor de PTS deve preencher todas as seções aplicáveis e enviar este documento conforme solicitado pelo comprador.

Parte 1. Fornecedor de PTS					
Nome da empresa:					
Nome do contato:			Título:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		Código postal:	
URL:					

Parte 2. Informações de aprovação do dispositivo

Para cada dispositivo aplicável, indique o status de envio de hardware e firmware como:

A: Não houve modificações nas versões de hardware ou firmware conforme listado no site do PCI;

B: Todas as alterações de hardware e firmware foram avaliadas por um laboratório de PTS em relatório apresentado à PCI, incluindo as versões de hardware ou firmware identificadas utilizando uma metodologia validada com versão variada (curinga).

Número de aprovação de PTS	Nome do modelo				
		Tipo A ou B	Versão do hardware	Versão do firmware	Versão do aplicativo (se aplicável)
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			

Parte 3. reconhecimento do fornecedor de PTS	
Assinatura do diretor executivo do fornecedor PTS ↑	*Data ↑*
Nome do diretor executivo do fornecedor PTS ↑	*Título ↑*
Empresa fornecedora de PTS representada ↑	