Industria de tarjetas de pago (PCI)

Seguridad de las transacciones con PIN (PTS)

Guía del programa de pruebas y aprobación de dispositivos

Versión 1.9

Junio de 2020

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción
Septiembre de 2010	1.0	Versión inicial
Octubre de 2011	1.1	Se agregaron clases de aprobación para el cifrado de lectores de tarjetas y dispositivos sin entrada de PED.
Julio de 2012	1.2	Se agregaron HSM v2 y aclaraciones sobre comisiones, clases de aprobación y fechas de vencimiento.
Septiembre de 2013	1.3	Actualización para POI v4 y aclaración sobre integración, protocolos abiertos, SRED, archivo de dispositivos, determinación de estado de aprobación, evaluaciones delta, plazos de presentación, comisiones, lectores de tarjetas seguros y dispositivos sin entrada de PIN.
Marzo de 2014	1.4	Se hicieron cambios en los requisitos de muestreo de dispositivos, así como adiciones al proceso de notificación de riesgos. Se definió una categoría nueva de dispositivos: *Dispositivos con aprobación vencida.* Se añadieron aclaraciones relativas a las características de las clases de aprobación—soporte de PIN, administración de claves y funciones proporcionadas—. Se actualizaron las definiciones de dispositivos sin entrada de PIN y SCR. Se añadieron explicaciones sobre el proceso de evaluación delta.
2015	1.5	Se modificó el proceso para solicitar el cambio de razón social/dirección/datos de contacto a través de un formulario de solicitud de cambio administrativo presentado al laboratorio; cambio en el ciclo de facturación; facturas prorrateadas emitidas el 1 de noviembre para todos los dispositivos listados entre el 2 de mayo y el 31 de octubre. Nueva guía sobre licencias (cambios de marca) del dispositivo de otro proveedor.
2016	1.6	Se actualizó para POI versión 5 y HSM versión 3. Se replantearon los plazos de prueba. Se agregó información sobre la clase de aprobación de HSM para dispositivos de carga de claves y plataformas de administración remota. Se hicieron aclaraciones sobre los tipos de productos OEM autónomos.
Mayo de 2017	1.7	Se agregó un requisito para modificar la política de seguridad para cambios administrativos. Se agregó texto para indicar cuándo se utiliza el Formato 4 de Bloqueo de PIN para el cifrado de PIN conforme a la ISO, en específico, la AES, y el método en el que se utiliza, es decir, DUKPT, clave fija o maestra/de sesión. Se actualizó el Apéndice B para POI versión 5.
Marzo de 2018	1.8	Se agregó la clase de aprobación SCRP, incluyendo especificaciones exclusivas para SCRP para nuevas aprobaciones y fechas de vencimiento. Se agregó el requisito de una certificación de validación anual respecto a los cambios en el firmware (Sección 3). Cambios en las pruebas de canal secundario. Se agregó el Apéndice D: Certificación de validación PTS. Erratas.

Fecha	Versión	Descripción
Junio de 2020	1.9	Se migraron las preguntas técnicas frecuentes relacionadas con el programa. Se actualizó el Apéndice D: "Certificación de validación PTS". Se agregó el Apéndice E: "Certificación de dispositivo PTS". Se eliminó el cuestionario para proveedores. Erratas.

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

Índice

1 Introducción

Las secciones siguientes presentan la información fundamental y de antecedentes de esta*Guía del Programa de pruebas de seguridad y aprobación de transacciones con PIN de PCI.*

1.1 Publicaciones relacionadas

Además de esta Guía del Programa (que describe el proceso de pruebas y aprobación), el marco de seguridad de las transacciones con PIN (PTS) del Consejo de Normas de Seguridad (SSC) de la Industria de Tarjetas de Pago (PCI) incluye los siguientes documentos:

Nota:*Estos documentos se actualizan y ratifican de manera rutinaria. Al utilizar estos requisitos, debe aplicar las versiones actuales. Las normas más actuales estarán disponibles en www.pcisecuritystandards.org.*

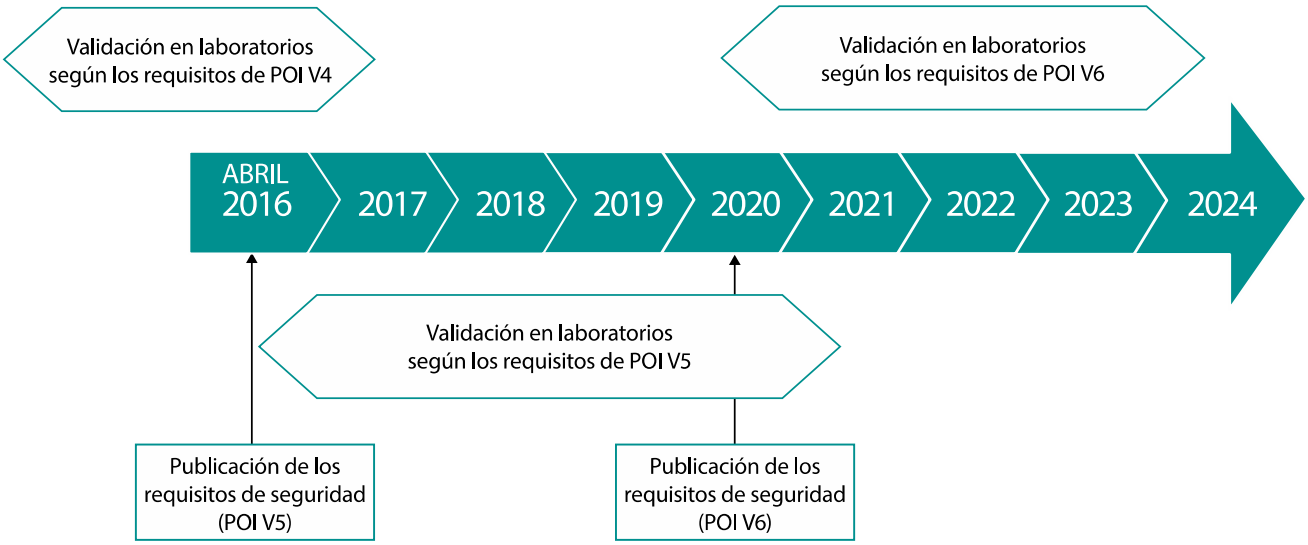
Nombre del documento	Descripción
Requisitos de seguridad	
▪ *Requisitos de seguridad modular del punto de interacción (POI) para la seguridad de transacciones con PIN (PTS), versión 6.0* ▪ *Requisitos de seguridad del módulo de seguridad de hardware (HSM) para la seguridad de transacciones con PIN (PTS), versión 3.0* ▪ *Requisitos de seguridad y procedimientos de prueba de PIN, versión 3.0*	POI y HSM contienen los requisitos físicos y lógicos de los dispositivos de seguridad, así como los de administración de dispositivos para actividades previas a la carga de la clave inicial. Entregue los formularios que utilizarán los laboratorios y los proveedores. PIN contiene un grupo completo de requisitos para la administración, procesamiento y transmisión seguros de datos del número de identificación personal (PIN) durante el procesamiento en línea y fuera de línea de transacciones con tarjetas de pago en cajeros automáticos y terminales de punto de venta (POS) asistidas y no asistidas.
Preguntas frecuentes	
▪ *PTS POI: Preguntas frecuentes*	Preguntas frecuentes generales.
▪ *Preguntas técnicas frecuentes sobre requisitos de seguridad de PTS POI para uso con la versión 6* ▪ *Preguntas técnicas frecuentes sobre requisitos de seguridad de PIN para PTS para uso con la versión 3* ▪ *Preguntas técnicas frecuentes sobre el módulo de seguridad de hardware (HSM) para uso con la versión 3*	Haga aclaraciones adicionales y oportunas sobre la aplicación de los requisitos de seguridad. Las preguntas frecuentes son parte integral de esos requisitos y deben considerarse cabalmente durante el proceso de evaluación.

Nombre del documento	Descripción
Cuestionarios de evaluación de proveedores	
▪ *Cuestionario de evaluación de proveedores sobre el módulo de seguridad de hardware (HSM) con seguridad de transacción con PIN (PTS), versión 3.0*	Solicite información adicional a los proveedores para que respalden sus afirmaciones sobre la conformidad de sus dispositivos con tales requisitos.
Requisitos derivados de la prueba	
▪ *Requisitos de prueba derivados del punto de interacción (POI) con seguridad para transacciones con PIN (PTS), versión 6.0* ▪ *Requisitos de prueba derivados del módulo de seguridad de hardware (HSM) para seguridad de transacciones con PIN (PTS), versión 3.0*	Dé a los proveedores instrucciones específicas sobre los métodos que pueden aplicar los laboratorios de pruebas para verificar el cumplimiento de los requisitos.
Lista de laboratorios reconocidos	
▪ *Laboratorios reconocidos por la Industria de tarjetas de pago (PCI)*	Laboratorios reconocidos en la actualidad para pruebas de dispositivos PTS.
Convenio de descargo del proveedor	
▪ *Convenio de descargo del proveedor de la industria de tarjetas de pago*	Contiene los términos y condiciones que rigen el intercambio de información entre proveedores y PCI SSC.
Lista de modelos de terminales aprobados	
▪ *Dispositivos de seguridad aprobados para transacciones con PIN*	Lista dispositivos de seguridad para transacciones con PIN aprobados por PCI SCC.

Los documentos arriba descritos están disponibles en la sección "Seguridad para transacciones con PIN" del sitio web de PCI SSC:www.pcisecuritystandards.org.Puede encontrar las versiones anteriores de los documentos en el archivo de documentos de seguridad para transacciones con PIN del mismo sitio web.

1.2 Actualizaciones de documentos y requisitos de seguridad

La seguridad es una carrera interminable contra los posibles atacantes. Por eso, es necesario revisar, actualizar y mejorar con frecuencia los requisitos de seguridad utilizados para evaluar los módulos de seguridad de los dispositivos POI y del hardware, a los que denominamos de manera colectiva como "dispositivos de seguridad de pago". Por lo tanto, PCI SSC ha convenido que todos los requisitos de seguridad pertinentes y los requisitos de prueba asociados se actualicen normalmente cada tres años. El siguiente diagrama describe el ciclo de tres años para la versión 5 de los Requisitos de Seguridad, las versiones anteriores y la versión 6.



PCI SSC se reserva el derecho de cambiar, enmendar o retirar requisitos de seguridad en cualquier momento. Si un cambio es necesario, PCI SSC se esforzará por trabajar de cerca con clientes[1] y proveedores para ayudar a reducir el impacto de los cambios.

[1] Los clientes son instituciones financieras que:

a) Ofrecen tarjetas de pago para una o más marcas de pago participantes (emisores);

b) Aceptan tarjetas de pago para desembolsos de efectivo y, directa o indirectamente, ingresan el recibo resultante de la transacción en intercambio (adquirentes); o bien,

c) Ofrecen servicios financieros a comerciantes o terceros autorizados que aceptan tales tarjetas de pago por mercancías, servicios, o desembolsos de efectivo y, directa o indirectamente, ingresan el recibo resultante de la transacción en intercambio (adquirentes).

De acuerdo con las disposiciones emitidas por las marcas de pago participantes, los clientes deben usar los resultados de las pruebas y aprobaciones del PCI SSC al tomar decisiones acerca de comprar dispositivos que han sido aprobados dentro del marco de PTS de PCI.

1.3 Acerca de este documento

La *Guía del Programa de pruebas y aprobación de dispositivos de seguridad para transacciones con PIN (PTS) de la Industria de tarjetas de pago* proporciona información para los proveedores respecto al proceso de evaluación y aprobación de PCI SSC de los dispositivos de seguridad para pagos, y refleja la conformidad de las marcas de pago con tarjeta participantes con un grupo estándar de:

- Requisitos de seguridad para el móduo de seguridad del punto de interacción (POI) y del hardware (HSM),
- metodologías de prueba y
- procesos de aprobación.

En este documento:

- "Participantes en PCI" y "marcas de pago participantes en PCI" se entenderán como cualquier entidad admitida en ese momento como miembro del Consejo de conformidad con la Ley de Sociedades de Responsabilidad Limitada de Delaware.
  Al día de hoy, los participantes en PCI son American Express Travel Related Services Company, Inc., DFS Services LLC (Discover), JCB Advanced Technologies, Inc., MasterCard International Incorporated, y Visa Holdings, Inc.
- "PCI SSC", "PCI" y "Consejo" se refieren a PCI Security Standards Council, LLC, sociedad de responsabilidad limitada constituida en Delaware por las marcas de tarjeta de pago antes mencionadas como "Participantes en PCI".
- "Dispositivos de punto de interacción (POI)" se refiere, en general, a todos los dispositivos con aceptación de PIN utilizados en transacciones con consumidores. Según se describe en el Apéndice A, el marco POI puede incluir otros tipos de dispositivos para transacciones con consumidores para abordar cualesquier amenazas emergentes al titular de la tarjeta o los datos sensibles de los participantes en PCI.
- Por "Módulos de seguridad de hardware (HSM)" se entiende los dispositivos criptográficos seguros utilizados para el procesamiento de PIN, personalización de tarjetas, administración de claves criptográficas y protección de datos.
- Por "Dispositivos de seguridad de pago" se entienden los dispositivos POI y HSM, de manera conjunta.
- "Seguridad de las transacciones con PIN" se refiere al marco dentro de las normas y requisitos de PCI que trata la evaluación y aprobación de dispositivos de seguridad de pago.

1.4 Acerca del PCI Security Standards Council

El Security Standards Council de la industria de tarjetas de pago (PCI) ha establecido el marco de seguridad para transacciones con PIN para abordar la evaluación de seguridad y aprobación de los dispositivos de seguridad de pago.

Esta *Guía del programa de pruebas y aprobación de dispositivos de seguridad para transacciones con PIN de la Industria de tarjetas de pago* refleja la conformidad con las marcas de pago participantes con un conjunto de:

- Requisitos de seguridad,
- metodologías de prueba y
- Procesos de aprobación

Nota:
Las aprobaciones se otorgan en forma directa a través de PCI SSC y las marcas de pago participantes en PCI las coordinan a través del proceso del programa PCI PTS.

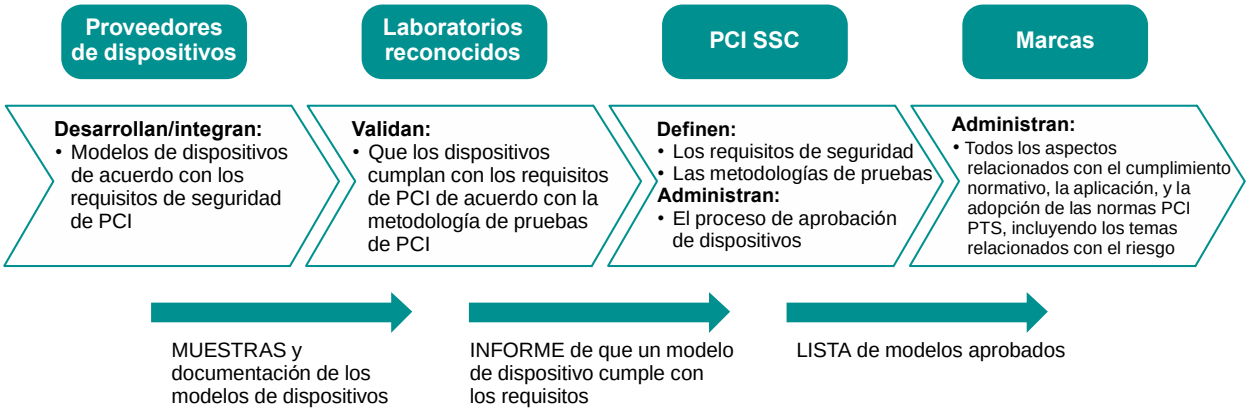
Todos los dispositivos presentados para evaluaciones de seguridad y aprobación han sido evaluados según los requisitos de seguridad PTS aplicables de la industria de tarjetas de pago (PCI). Las listas de aprobación de PCI proporcionan una lista completa de los dispositivos de seguridad de pago que cuentan con reconocimiento por cumplir con los requisitos de PCI PTS.

Este esfuerzo colaborativo garantiza que todos los dispositivos de seguridad de pago se evalúen conforme a un proceso común que ofrece un nivel alto de seguridad. Este acuerdo tiene la intención de mejorar la seguridad general para el titular de la tarjeta y otros datos sensibles eliminando requisitos que se encuentren en conflicto. Todos los stakeholders en la cadena de valor de pagos se benefician de los requisitos alneados:

- Los clientes se benefician con una selección más amplia de dispositivos seguros.
- Los comerciantes, instituciones financieras, procesadores y otros terceros tienen la seguridad de que están usando productos que han cumplido con el nivel necesario de garantía.
- Los proveedores pueden reducir el "tiempo de lanzamiento al mercado" de sus dispositivos nuevos, ya que solo deberán completar una sola evaluación de seguridad y un solo proceso de aprobación.

1.5 Normas de marcas de pago

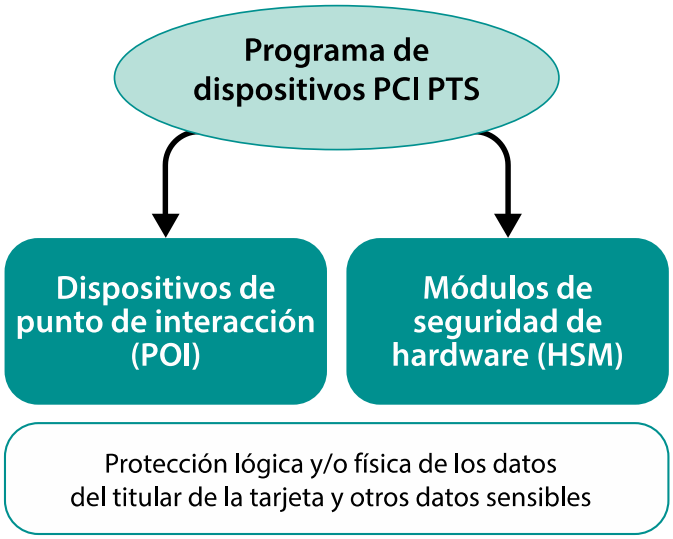
Todos los aspectos relacionados con el cumplimiento, aplicación y adopción de estas normas, incluyendo todos los asuntos relacionados con el riesgo son responsabilidad de las marcas individuales de tarjeta de pago. La siguiente imagen ofrece una descripción de alto nivel de la cadena de seguridad del dispositivo.



2 Descripción del proceso de pruebas y aprobación

2.1 Descripción general

El marco de aprobación de seguridad de PCI SCC PTS aborda la protección lógica y/o física del titular de la tarjeta y otros datos sensibles en los dispositivos del punto de interacción (POI) y los módulos de seguridad de hardware (HSM), como lo indica el siguiente diagrama.



Salvo que se indique lo contrario, este documento designa los dispositivos POI y HSM como "dispositivos de seguridad de pago".

Los proveedores de dispositivos que deseen que PCI SSC apruebe sus modelos de dispositivo pueden comunicarse con uno de los laboratorios reconocidos por PCI y llenar los formularios PCI adecuados (incluidos en los*requisitos de seguridad de PCI PTS*). El proveedor presentará el dispositivo, junto con cualquier documentación adicional solicitada por el laboratorio, para su evaluación y validación de cumplimiento conforme a los requisitos de seguridad PCI PTS. Una vez concluida la evaluación, PCI SSC revisará el informe de evaluación. Cuando el modelo del dispositivo cumpla con los requisitos de PCI, será aprobado y listado en el sitio web de PCI PTS. Se emitirá una carta de aprobación confirmando la conclusión satisfactoria del proceso.

2.2 Antes de las pruebas (solo para dispositivos POI)

- PCI SSC recomienda que el dispositivo POI reciba primero una aprobación EMV nivel 1, si fuese el caso, y luego la aprobación PCI, antes de presentarlo para cualquier prueba EMV de nivel 2. (Con respecto a la aprobación EMV nivel 1, debe haber poca superposición, o ninguna, en los procesos de prueba y la aprobación de seguridad de PCI PTS POI).
- Si el dispositivo POI es compatible con ambos tipos de opciones de entrada de PIN, en línea y sin conexión, informe al laboratorio para que evalúe ambas al mismo tiempo o que el laboratorio indique la compatibilidad futura para ambas opciones en el informe de evaluación. Para que la aprobación del dispositivo POI indique la compatibilidad de ambas opciones, el proveedor debe asegurarse de que después de realizar la evaluación de la segunda opción de entrada de PIN, el laboratorio incluya ambas en el informe.

2.3 El enfoque modular

El enfoque modular de PCI PTS ofrece un proceso de evaluación integral que aborda la diversidad de arquitecturas, opciones de producto y modelos de integración de los dispositivos de seguridad de pago. Optimiza en forma potencial los costos de evaluación y el tiempo en que los laboratorios revisan las arquitecturas no convencionales, la aprobación de PCI de los tipos de productos, y el mantenimiento de las aprobaciones existentes (cambios en los componentes de seguridad, etc.).

El enfoque modular de PCI PTS admite la presentación de dispositivos conforme al tipo de producto y las clases de aprobación definidas en el Apéndice A.

Cuadro 1: Módulos de evaluación

Para que el laboratorio capture la diversidad de requisitos de seguridad en un solo proceso de evaluación de cumplimiento, los requisitos de seguridad de PTS de POI se dividen en los siguientes módulos de evaluación:

Requisitos y nombre del módulo de evaluación	Descripción
Seguridad física	Requisitos de seguridad física de los dispositivos POI
Seguridad lógica	Requisitos de seguridad lógica de los dispositivos POI
Requisitos de integración del dispositivo	Garantiza que la integración de los componentes aprobados con anterioridad no merme la seguridad general establecida en los requisitos de seguridad e incluye requisitos de administración de seguridad aplicables al dispositivo integrado.
Comunicaciones e interfaces	Interfaz de terminales POI para abrir redes que utilizan protocolos abiertos.
Ciclo de vida	Considera la manera en que se produce, controla, transporta, almacena y utiliza el dispositivo a lo largo de su ciclo de vida.

Cualquier producto que incorpora módulos separados, como un EPP, lectores de tarjeta, etc., debe cumplir los requisitos de integración.

Los productos compatibles con protocolos abiertos o que buscan tener una designación de lectura e intercambio seguros de datos (SRED)deben evaluarse según los requisitos de seguridad pertinentes mencionados en el Apéndice B: Aplicabilidad de los requisitos en *Requisitos de seguridad modular del POI para PTS*. Consulte las columnas "Implementación de protocolos abiertos" y "Protección de los datos de cuentas" para conocer los requisitos que deben cumplirse además de otros aplicables.

Cualquier método de comunicación que utilice una red inalámbrica, local o de área amplia para transportar datos está sujeto a evaluación de protocolos abiertos. Esto incluye, entre otros, Bluetooth, Wi-Fi, celular (GPRS, CDMA) o Ethernet. No se requeriría evaluar una conexión en serie punto a punto salvo que la conexión sea inalámbrica o a través de un concentrador, conmutador u otro dispositivo de varios puertos. Además, cualquier comunicación que utilice un protocolo de dominio público o protocolo de seguridad también se evaluaría con los requisitos aplicables a los protocolos abiertos.

Existen varias situaciones donde SRED es obligatorio. Estas situaciones incluyen cualquier dispositivo validado para las clases de aprobación que no sean PED o SCR, o en algunas situaciones de dispositivos portátiles que involucran un dispositivo con entrada de PIN conectado (p. ej., por deslizamiento, cubierta o audio jack) a un teléfono móvil, PDA o terminal POS.

La intención general del requisito de validación de SRED es garantizar que la implementación de la protección de datos de cuentas es completamente sólida según se demuestra por validación y aprobación según los requisitos SRED. No obstante, el requisito no tiene la intención de que el proveedor no implemente protecciones de datos de cuenta que no sean suficientes para cumplir con los requisitos SRED aplicables, sino que ofrece un nivel menor de protección para los datos de cuenta. Así, un proveedor que implemente protecciones de datos de cuenta y ***no*** busque SRED como una función aprobada puede hacerlo de esta manera.

2.4 Proceso de pruebas

Los dispositivos de seguridad de pagos se evalúan utilizando los requisitos incorporados en los *Requisitos de seguridad modular del POI para PTS* o el manual de *Requisitos del módulo de seguridad de hardware de PCI* ("Manual HSM"), según sea el caso. El laboratorio verificará las respuestas "SÍ" y "N/A" del proveedor en esas secciones haciendo que el proveedor entregue pruebas adicionales de conformidad con los requisitos según lo declarado por medio de información y muestras requeridas del dispositivo de seguridad de pagos. No se aceptarán informes con un "No" como respuesta.

Cualquier producto que incorpora módulos separados, como EPP, lectores de tarjeta, etc., debe cumplir los requisitos de integración. Los productos no están obligados a admitir protocolos abiertos o lectura e intercambio seguros de datos; sin embargo, si lo hacen, tales requisitos son obligatorios para la evaluación y aprobación.

Los fabricantes de terminales pueden comprar componentes seguros aprobados por PCI a varios proveedores e integrarlos en sus soluciones finales que ellos mismos pueden aprobar según los requisitos de PTS de PCI.

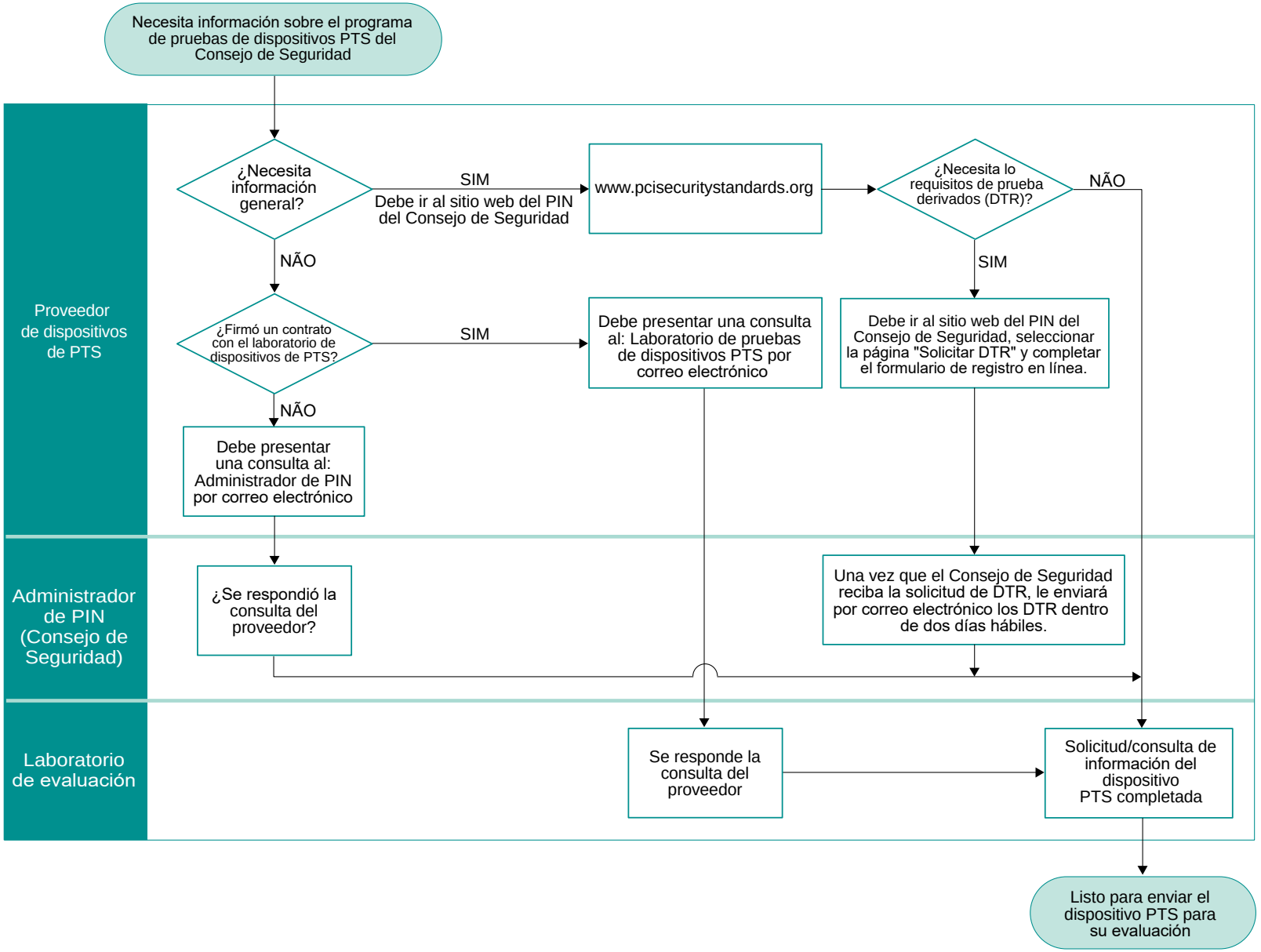
El laboratorio validará los dispositivos de seguridad de pagos según los Requisitos de ciclo de vida especificados en los *Requisitos de seguridad modular del POI para PTS de PCI* o *los Requisitos de seguridad de PCI sobre HSM.* Esto se hace a través de revisiones de documentación y por medio de pruebas de que el procedimiento se implementó y se utiliza en forma adecuada. Cualquier variación de estos requisitos se informará a PCI para que se revise. Esta información se requiere como parte del proceso de aprobación.

Cuadro 2: Ilustración de las pruebas y el proceso de aprobación

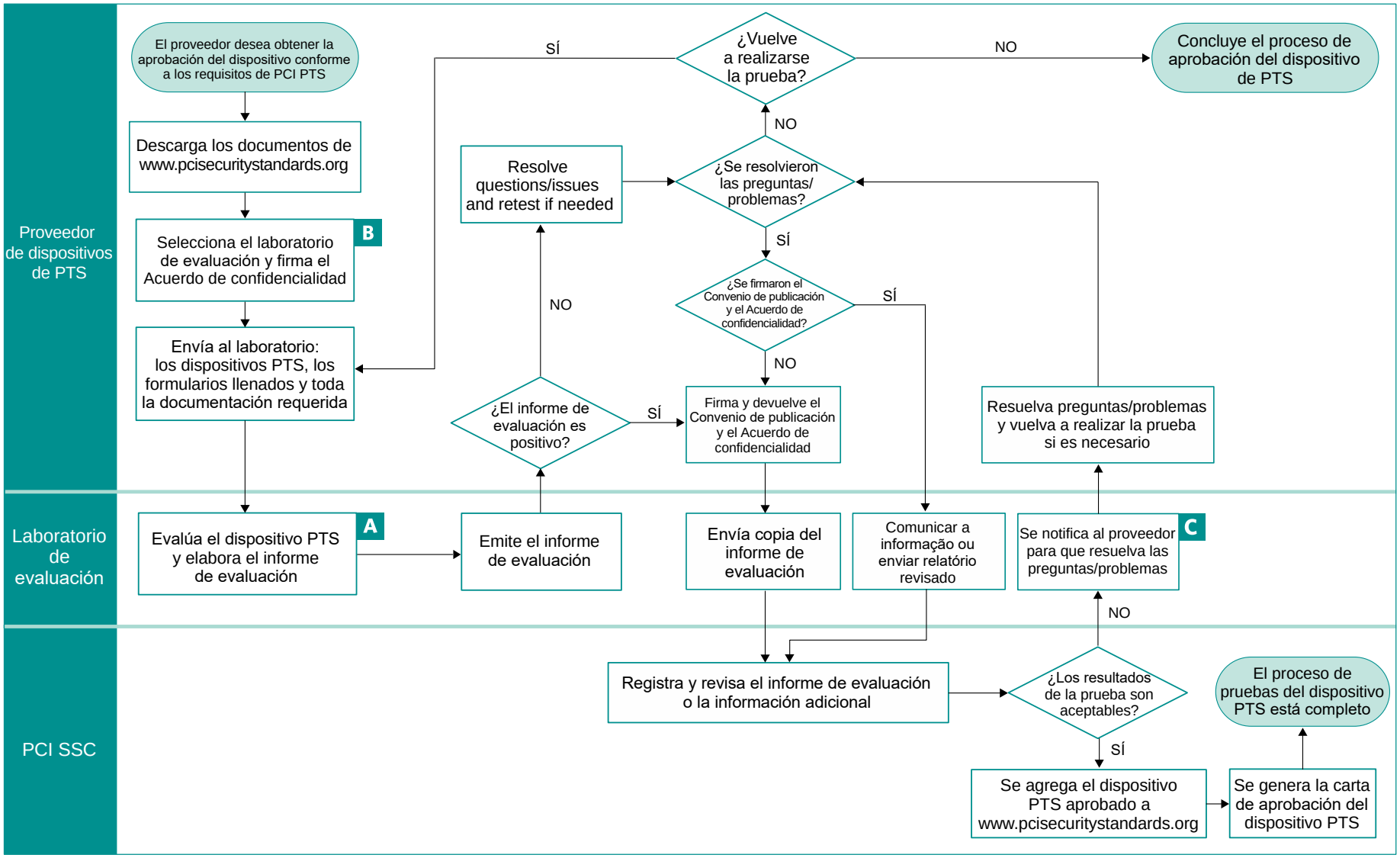
El siguiente cuadro y los gráficos en las hojas a continuación describen e ilustran el proceso de pruebas y aprobación del dispositivo de seguridad de pagos.

Etapa del proceso	Recurso/Explicación	Ilustración
Antes de las pruebas	Descripción del proceso de pruebas y aprobación	Figura 1
Obtener los documentos y formularios adecuados	Proceso detallado de evaluación	Figura 2
Comunicarse con un laboratorio de pruebas reconocido por PCI para iniciar las pruebas	Preparación para las pruebas	Figura 2
Firmar el contrato de confidencialidad y el convenio de descargo	Proceso de aprobación	Figura 2
Presentar la documentación y los materiales	Requisitos para las pruebas	Figura 2
Responder los cuestionarios del laboratorio de pruebas	Soporte técnico durante las pruebas	Figura 2
Recibir la respuesta o carta de aprobación del PCI SSC	Proceso de aprobación	Figura 2
Cambios en el dispositivo de PTS	Cambios a un dispositivo PTS previamente aprobado	Figura 3

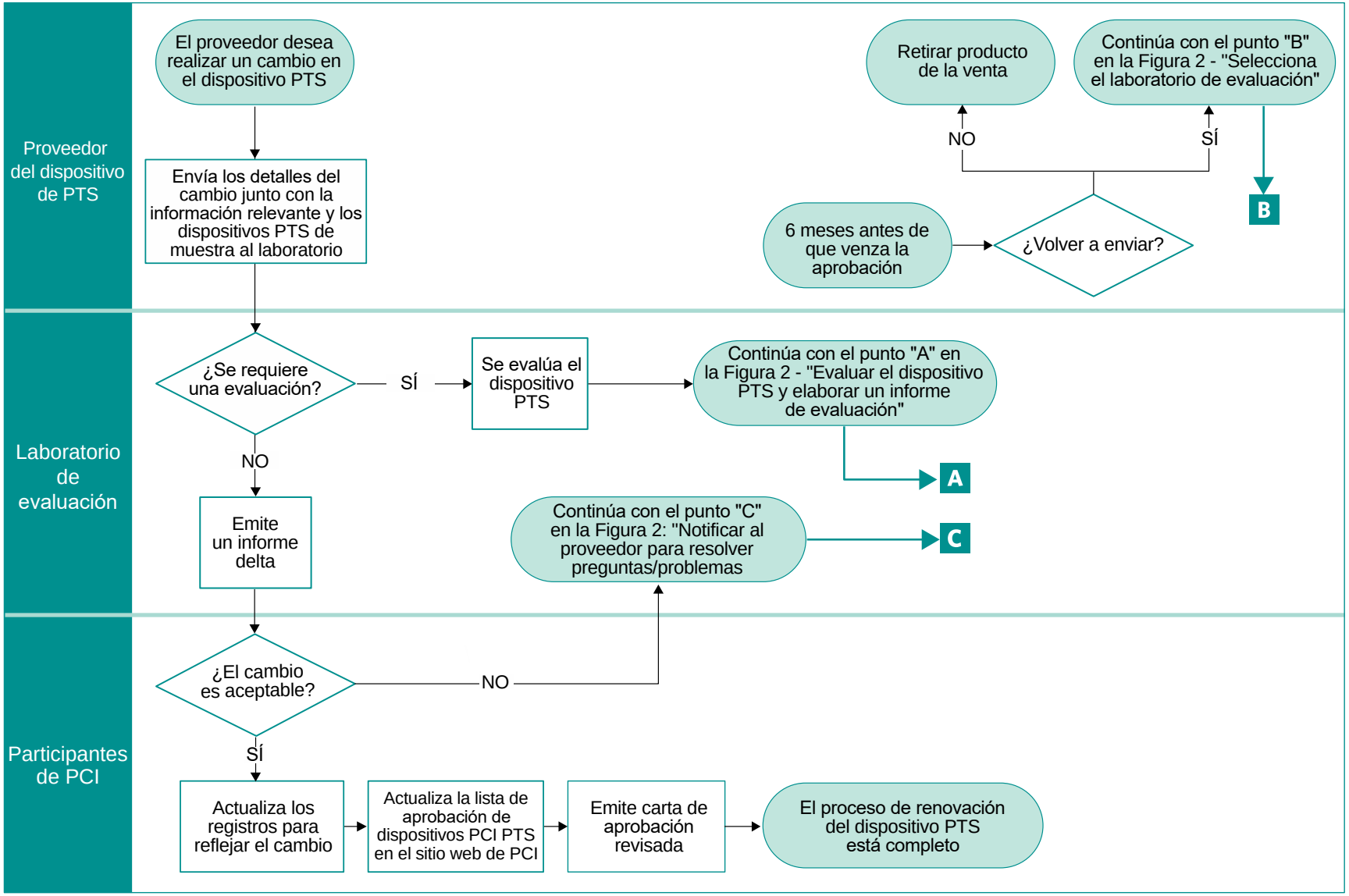
2.5 Figura 1: Diagrama de flujo de la investigación para pruebas de dispositivos PTS



2.6 Figura 2: Diagrama de flujo de la aprobación para dispositivos PTS



2.7 Figura 3: Diagrama de flujo de la solicitud de un cambio o renovación de un dispositivo de PTS



3 Proceso detallado de evaluación

Los dispositivos de seguridad de pagos se evaluarán según los *Requisitos de seguridad modular del POI para PTS de PCI* o el manual de *Requisitos de seguridad del módulo de seguridad de hardware de la Industria de tarjetas de pago*. El laboratorio evaluará las respuestas del proveedor en esas secciones haciendo que el proveedor entregue pruebas adicionales de la conformidad con los requisitos, a través de información y muestras del dispositivo requerido de seguridad de pagos. El PCI SSC revisará el informe adecuado de la evaluación del dispositivo de seguridad de pagos que entregue el laboratorio. Si los resultados son satisfactorios, se aprueba el dispositivo de seguridad de pago y el dispositivo de PTS se publica como un dispositivo de seguridad de pago "aprobado por PCI" en www.pcisecuritystandards.org. Luego, se emitirá una carta de aprobación a favor del proveedor.

Las preguntas técnicas frecuentes son parte integral del proceso de evaluación. Las preguntas técnicas frecuentes se identifican por versión principal de los requisitos de seguridad, p. ej., 4.x, 5.x, 6.x. Cada versión de las preguntas técnicas frecuentes es específica para la versión principal correspondiente de los requisitos de seguridad. Por ejemplo, la versión 6 de las preguntas técnicas frecuentes es específica para la versión 6.x de los requisitos de seguridad y solo la versión 6.x de los requisitos de seguridad, y así sucesivamente.

Las preguntas técnicas frecuentes se actualizan de manera periódica y, en general, entran en vigor a partir de su publicación. Dependiendo de la naturaleza de las preguntas frecuentes (p. ej., aclaración frente a tratamiento de una amenaza eminente), su aplicabilidad puede diferir para los dispositivos que se evalúan a momento de la publicación.

Las modificaciones a los dispositivos aprobados, denominadas "deltas", pueden ocurrir en cualquier momento durante la aprobación del producto. Los dispositivos que se sometan a evaluaciones de delta deben tomar en cuenta las Preguntas frecuentes actuales de la versión principal de los requisitos de seguridad solo de los requisitos de seguridad que resultan afectados por la delta. Por ejemplo, si un cambio afecta el cumplimiento con los requisitos B1 y B4, solo deben tomarse en cuenta las Preguntas frecuentes asociadas con B1 y B4 como parte de la delta.

Los dispositivos cuya aprobación venció también pueden someterse a deltas. Esto se debe a que posiblemente los proveedores tengan que hacer arreglos de mantenimiento a los dispositivos que el proveedor ya haya vendido, pero para los que todavía debe proporcionar soporte técnico. Además, es posible que los proveedores deseen transferir versiones actualizadas de firmware aprobadas conforme a requisitos de seguridad más actuales a productos cuya aprobación ha vencido Esto puede suceder cuando los clientes de un proveedor desean estandarizar sus implementaciones de acuerdo con una versión específica de firmware y/o agregar funciones a esos dispositivos.

A partir de la publicación de una versión nueva importante (p. ej., 4.x, 5.x, 6.x) habrá un periodo de doce meses de superposición con la versión existente, a partir del mes del año en que se publique la versión principal más reciente. Durante ese periodo, los proveedores pueden elegir si presentan un dispositivo conforme a cualquiera de las versiones de los requisitos de seguridad. La excepción es SCRP cuyas aprobaciones nuevas siempre deben utilizar la versión más actual de los requisitos de seguridad. Doce meses después de la publicación de la versión principal nueva, la versión anterior de los requisitos de seguridad solo estará disponible para las evaluaciones de deltas.

En el año anterior a que los requisitos se retiren de uso, cualquier proveedor que utilice tales requisitos para una evaluación nueva deberá tener el dispositivo en evaluación sesenta días antes de la fecha de retiro de la versión, y cada laboratorio reconocido por PCI notificará a PCI por escrito sobre los dispositivos específicos que tengan en evaluación. PCI deberá recibir los informes definitivos de evaluación del laboratorio al final de dicho plazo de sesenta días. Si los dispositivos requieren cambios con base en la revisión que PCI haga de los informes de evaluación, dichos cambios podrán hacerse después del plazo de sesenta días. Sin embargo, PCI no aceptará ningún informe de evaluación revisado después de un periodo de sesenta días a partir del retiro de la versión principal anterior.

A partir del 31 de enero, el proveedor debe llenar y presentar ante PCI una Certificación de Validación (AOV – véase el Apéndice D) donde confirme su apego a la guía del programa, es decir, ya sea que el firmware no tiene modificaciones o que los cambios se hicieron conforme a los parámetros comodín o se presentaron para evaluación. El proceso de vulnerabilidad reportado en la AOV debe incluir todas las interfaces físicas y sus protocolos lógicos correspondientes según se definen en el D1. Para los dispositivos compatibles con protocolos abiertos, el proveedor deberá entregar materiales probatorios de que existe un registro auditable del proceso de evaluación de vulnerabilidades en curso proporcionando una copia del formulario de aprobación del proveedor especificado en el Requisito E10. Esto se aplica a todas las aprobaciones sin vencer que existan para el proveedor al 31 de diciembre del año anterior. Si no se presenta la AOV anual, no se procesarán los demás informes que presente el proveedor. No se requiere una AOV para los dispositivos que se encuentren al final de su vida útil que se enumeran en la Sección 5.

A partir del POI v6., el firmware vence el 31 de diciembre cada tres años subsiguientes al año de aprobación inicial. Por ejemplo, las versiones de firmware aprobadas durante 2020 vencerán e 31 de diciembre de 2022, el 31 de diciembre de 2025, y el 31 de diciembre de 2028. Este vencimiento es independiente de la fecha de vencimiento general del dispositivo —véase la Sección A.12—. El laboratorio debe evaluar el firmware restante sin vencer conforme a los siguientes DTR, y presentará un informe a PCI, quien dará su aprobación, antes del 1 de mayo del año siguiente al vencimiento:

Nota:
Esta evaluación es adicional a la AOV anual.

DTR B16	Separación de aplicaciones
DTR B17	Configuración mínima
DTR B22	Acceso remoto
DTR D2	Anomalías lógicas
DTR E10	Procedimientos de evaluación de vulnerabilidades de proveedores
DTR E11	Evaluación de vulnerabilidades de todas las interfaces
DTR E12	Divulgación de vulnerabilidades

Asimismo, las entidades que compran los dispositivos pueden pedir a los proveedores que llenen una Certificación de dispositivo PTS —véase el Apéndice E—. Este documento es para que los proveedores certifiquen que las versiones del hardware y del firmware de los dispositivos se compran de conformidad con los números de versión listados en el sitio web de PCI para ese modelo o número específicos de dispositivo.

3.1 Documentación y materiales requeridos

Toda la información y documentos pertinentes al programa de pruebas y aprobación de PTS de PCI pueden descargarse en www.pcisecuritystandards.org. Todos los formularios y cuestionarios llenos relacionados con la evaluación de los dispositivos de seguridad de pagos deben entregarse al laboratorio de pruebas reconocido por PCI, no al PCI SSC. La información específica de la evaluación se solicita directamente al laboratorio reconocido por PCI.

Estos son algunos ejemplos de los documentos y artículos que deben presentarse al laboratorio de pruebas de dispositivos de seguridad de pagos reconocido por PCI para la clase de aprobación del dispositivo:

1. Formularios de los *Requisitos de seguridad de PCI* para el dispositivo, llenados de manera adecuada.
2. Cuestionario del proveedor de laboratorio llenado para el dispositivo.
3. Una política de seguridad disponible para el usuario para publicar con la aprobación en www.pcisecuritystandards.org. El documento debe contener, como mínimo, la información prescrita en los requisitos de prueba derivados aplicables.
4. Tres (3) dispositivos POI funcionales (para HSM, se debe consultar al laboratorio) con el manual del operador o instrucciones. Además, para los dispositivos POI que se sometan a evaluaciones nuevas, e proveedor debe entregar dos dispositivos funcionales al laboratorio para archivo en PCI como se indica a continuación.
5. Los accesorios de hardware y software necesarios para realizar las transacciones simuladas de pago con PIN (para HSM, se debe consultar al laboratorio).
6. La documentación que describa todas las funciones utilizadas para la entrada y salida de datos que puedan utilizar terceros desarrolladores de aplicaciones. En específico, debe describir las funciones relacionadas con la administración de claves, administración de PIN, e interfaces de usuario (como pantalla y teclado). (Un manual de la API es un ejemplo de documentación que pudiera cumplir con este requisito.)
7. La documentación que se relaciona con el "proceso que se auditará". Estos son algunos ejemplos de tal documentación:
    - Procedimientos de calidad del software
    - Documentación y procedimientos de control de software
    - Formularios de cambios
    - Registros de control de cambios
    - Registros de cambios
8. Instrucciones y accesorios (como cargadores de claves) que permitan a los ingenieros del laboratorio de pruebas utilizar todos los modos especiales compatibles con el dispositivo de seguridad de pagos, incluyendo selección de claves, borrado de la clave por llenado con ceros, y otras funciones de administración y mantenimiento de claves.
9. Documentos adicionales, como (a) diagramas de bloque, esquemas y diagramas de flujo que ayudarán en la evaluación del dispositivo de seguridad de pago, y (b) factor de forma del dispositivo e imágenes relacionadas (si está aprobado por el PCI SSC) para su publicación en la lista de aprobación de dispositivos de PTS y uso relacionado del PCI SSC. En caso necesario, el laboratorio puede pedir material adicional para evaluación.

Lo siguiente se aplica solo a los dispositivos POI:

Después de una evaluación exitosa, el laboratorio de pruebas de PTS debe entregar dos muestras del dispositivo al Consejo. A continuación se indican la dirección de envío y contacto local. Se deben conservar los datos experimentales de ciertas pruebas realizadas para disposición futura del Consejo según sea necesario. Esto se aplica a todas las evaluaciones nuevas que originen un número nuevo de aprobación. Esto no se aplica a las deltas. Tampoco se aplica a una situación donde el proveedor solo está cambiando la marca de un producto aprobado con anterioridad de otro proveedor. Sin embargo, sí se aplica si un proveedor está cambiando la marca de un producto y, además, hace otros cambios, como en el firmware. Los datos adicionales y actualizaciones sobre estos asuntos estarán disponibles en comunicaciones de PCI a los laboratorios y proveedores. Se resumen como sigue:

- **Muestras de dispositivos:** Dos (2) terminales que contengan las mismas claves y aplicaciones que las proporcionados al laboratorio reconocido por PCI. Esto incluye todas las clases de aprobación. Notifique a los datos de contacto antes de enviar artículos grandes. Si un dispositivo tiene variantes diferentes, el laboratorio enviará dos variantes diferentes, seleccionando las dos más representativas del rango de todas las variantes. La entrega de muestras de dispositivos es una parte necesaria de la aprobación del dispositivo. Estas se mantendrán en forma segura y podrán utilizarse para evaluar la vulnerabilidad a técnicas nuevas de ataque. Si, alguna vez, un modelo se ve en riesgo en el campo, las muestras retenidas podrán utilizarse para investigar cualquier riesgo o vulneración de seguridad.
- **Las pruebas de canales secundarios sólidas** son una parte importante de la evaluación del dispositivo. El laboratorio debe almacenar los datos relevantes de la prueba de canal secundario (formas de ondas representadas digitalmente y datos numéricos asociados) producidos por una evaluación durante seis meses, por lo menos, después de la aprobación del dispositivo. El Consejo solicitará que se le entreguen algunos datos o todos los datos, según sea necesario. Los laboratorios deben comunicarse con el Consejo para resolver cualquier duda al respecto.
- **Las pruebas de anomalías lógicas sólidas** son una parte importante de la evaluación del dispositivo. Los informes de evaluación adjuntos deben presentar los ejemplos pertinentes de datos de exploración de vulnerabilidades (datos de salida y/o registros, informes, etc.), que ofrecen un resumen representativo y comprensible de las ejecuciones de pruebas de ataque para exploración de vulnerabilidades indicando qué prueba se realizó y el motivo, y detalles suficientes para explicar la justificación de las pruebas y las conclusiones.

Enviar los dispositivos a:	Información de contacto para el envío:
A la atención de: MasterCard Global Products and Solutions MasterCard Worldwide 5 Booths Park Chelford Road Knutsford Cheshire WA16 8QZ Reino Unido	Contacto: Deborah Corness Teléfono: +44 (0)1565 626500 Fax: +44 (0)7738 202 663 Correo electrónico: deborah_corness@mastercard.com

4 Preparación para las pruebas

4.1 Servicios de laboratorio

Un laboratorio reconocido por PCI puede ofrecer los siguientes servicios para facilitar el proceso de evaluación antes de la prueba real:

- Orientación en el diseño de dispositivos de seguridad de pagos para que se apeguen a los requisitos de seguridad de PCI.
- Revisión del diseño del dispositivo de seguridad de pagos del proveedor, respuesta a las preguntas por correo electrónico o teléfono y participación en conferencias telefónicas para aclarar los requisitos.
- Una evaluación preliminar de la seguridad física del hardware del proveedor.
- Guía para que los dispositivos de seguridad de pagos de un proveedor cumplan con los requisitos de PCI si, durante la evaluación, se identifican áreas de incumplimiento.

Se exhorta a los proveedores a que se comuniquen directamente con un laboratorio reconocido por PCI en relación con los servicios arriba mencionados y cualquier cuota relacionada con los mismos. Sin embargo, los laboratorios **no pueden** ofrecer ningún consejo sobre el diseño real del dispositivo POI o HSM.

4.2 Laboratorios reconocidos por PCI

En la actualidad, el PCI SSC reconoce una serie de laboratorios para pruebas de dispositivos de PTS. La lista vigente de los laboratorios de pruebas de PTS reconocidos se encuentra en el sitio web del PCI SCC, en la sección "Dispositivos de PTS aprobados".

4.3 Tarifas de pruebas

El proveedor y el laboratorio negociarán todas las tarifas y fechas relacionadas con las pruebas, y el proveedor pagará todas las tarifas directamente al laboratorio. Si se necesita que el proveedor modifique el diseño físico de un dispositivo de seguridad de pago o el firmware debido a alguna discrepancia, el dispositivo de seguridad de pago deberá presentarse otra vez para un ciclo nuevo de pruebas y el laboratorio facturará al proveedor lo que corresponda.

Nota:

El proveedor paga todas las tarifas de evaluación del laboratorio directamente a este.

4.4 Requisitos para las pruebas

Como requisito para las pruebas, el proveedor del dispositivo de seguridad de pago debe entregar la documentación adecuada y las muestras al laboratorio. Si requiere más información, consulte la sección "Documentación y materiales requeridos".

El laboratorio de pruebas puede realizar una evaluación previa de un dispositivo de seguridad de pagos de un proveedor y decidir si existen deficiencias que impedirían su aprobación. El laboratorio puede responder al proveedor con una lista de todos los aspectos del dispositivo de seguridad de pagos que deben abordarse antes de iniciar el proceso formal de pruebas.

4.5 Fechas de las pruebas

El laboratorio asignará una fecha de prueba a los proveedores que presenten dispositivos para pruebas en un laboratorio reconocido por PCI. Los proveedores deberán notificar al laboratorio en forma directa sobre cualquier demora en la presentación de dispositivos de seguridad de pagos para sus pruebas.

4.6 Plazos de pruebas

En general, una evaluación nueva puede empezar en un periodo dos semanas a partir de que el laboratorio reciba todos los artículos para prueba. Los intervalos de tiempo deben programarse con el laboratorio de manera anticipada. El tiempo real de evaluación variará según el alcance de la evaluación y la presteza del proveedor. La evaluaciones pueden realizarse con mayor rapidez si el laboratorio tiene toda la documentación requerida y el hardware, y si no hay problemas importantes de cumplimiento.

Los plazos de pruebas son cálculos basados en la suposición de que el dispositivo de seguridad de pagos complete la prueba de manera correcta. Si se encuentran problemas durante las pruebas, el laboratorio y el proveedor discutirán los asuntos que sean necesarios. Tales discusiones podrían afectar los plazos de pruebas y causar demoras y/o terminar el ciclo de prueba antes de concluir todas las pruebas.

4.7 Definición del ciclo de pruebas

Se requiere que todos los dispositivos de seguridad de pagos concluyan el ciclo de pruebas con resultados exitosos como parte del programa de pruebas y aprobación de PCI. Un **ciclo de pruebas**se define como la conclusión de todos los procedimientos de prueba aplicables llevados a cabo en una sola versión del dispositivo de seguridad de pagos del proveedor. Cuando se concluye un solo ciclo de pruebas sin discrepancias, se avisa al proveedor que el dispositivo de seguridad de pagos ha concluido el ciclo de pruebas con éxito.

Durante el proceso de pruebas, todos los procedimientos de prueba aplicables se ejecutan conforme a los *Requisitos de prueba derivados de PCI* aplicables. Se informará al proveedor sobre cualquier discrepancia encontrada. Todas las pruebas aplicables deben ejecutarse durante un solo ciclo de pruebas, salvo que:

- Un error de aplicación provoque que todas las pruebas en una porción del código lógico de software funcionen de manera incorrecta, lo que evita que se realicen más pruebas dentro del área de la aplicación.
- El dispositivo de seguridad de pagos contenga una falla catastrófica que evite cualquier continuación de la prueba.
- Las pruebas excedan la duración del ciclo de pruebas programado.
- El proveedor solicite la terminación del ciclo de pruebas.

Si un ciclo de pruebas ha terminado con discrepancias, se notifica al proveedor que el dispositivo de seguridad de pagos no pasó el ciclo de pruebas. El laboratorio emitirá un informe final que aborde las discrepancias.

No existe una disposición para interrumpir el ciclo de pruebas y volver a iniciarlo en una fecha posterior.

4.8 Soporte técnico durante las pruebas

El laboratorio, a su juicio, podrá solicitar información adicional al proveedor para poder resolver la discrepancia. Si se necesita que el proveedor modifique el diseño físico de un dispositivo de seguridad de pago o el firmware debido a alguna discrepancia, el dispositivo de seguridad de pago deberá presentarse otra vez para un ciclo nuevo de pruebas y el laboratorio facturará al proveedor lo que corresponda.

Se recomienda que el proveedor ponga a disposición a un técnico para que ayude con cualquier cuestión que pudiese surgir durante la prueba de laboratorio. Durante la evaluación, y para que el proceso sea expedito, el contacto del proveedor estará "de guardia" para discutir las discrepancias y responder a las preguntas del laboratorio.

El trabajo de evaluación del laboratorio se realizará utilizando personal y equipo aprobados del laboratorio. Las pruebas del dispositivo para las aprobaciones PTS se harán dentro de las instalaciones del laboratorio reconocido por PCI y no en el sitio del proveedor, salvo que:

- El trabajo del laboratorio se relacione con la evaluación de las políticas y procedimientos del proveedor.
- Se evalúen los requisitos de seguridad de ciclo de vida.
- Cuando sea necesario, se revise el código fuente.

Cualquier trabajo terminado fuera de la instalación del laboratorio reconocido por PCI debe documentarse en forma clara en el informe de evaluación del dispositivo de PTS de PCI.

5 Tarifas de PCI

Se cobra una tarifa a los proveedores por cada informe nuevo de evaluación que reciben. Además, se cobrará a los proveedores una tarifa de listado anual o mantenimiento por cada aprobación de PCI existente. Estas tarifas se estipulan en www.pcisecuritystandards.org/fees.

5.1 Morosidad

PCI no procesará ningún informe de los proveedores que sean morosos en sus pagos al PCI SSC hasta que se pongan al corriente. Asimismo, el PCI SSC podrá cobrar sanciones, tarifas e intereses a los proveedores morosos.

5.2 Nuevas evaluaciones

La tarifa de evaluaciones nuevas será una tarifa de transferencia del laboratorio de prueba aplicable al proveedor. El laboratorio de prueba entregará el dinero al PCI SSC y recuperará tales tarifas como parte de la tarifa de evaluación. La tarifa se facturará trimestralmente para todas las evaluaciones nuevas presentadas por el laboratorio en los tres meses precedentes. No se facturará a los proveedores por la modificaciones de hardware o firmware en aprobaciones de PCI existentes denominadas como aprobaciones "delta".

5.3 Evaluaciones iniciales conforme a las versiones principales

Todas las evaluaciones iniciales en virtud de una versión principal (p. ej., 5.x, 6.x, etc.) de los requisitos de seguridad de un producto dado deberán constituir una nueva evaluación y deberán recibir un nuevo número de aprobación y facturarse según corresponda. Las evaluaciones de deltas no pueden considerar un producto aprobado previamente en virtud de una virtud principal anterior, p. ej. 5.x para una aprobación conforme a otro número de versión principal, p. ej. 6.x.

5.4 Tarifa de listado de aprobación

El PCI SSC facturará la tarifa de lista de aprobación semestralmente. Las fechas de facturación se establecerán el 1 de mayo y 1 de noviembre de cada año. Se facturará a los proveedores el monto total de todas las aprobaciones de PCI existentes y en vigor el 30 de abril para cubrir el periodo del 1 de mayo al 30 de abril. La facturación del 1 de noviembre cubrirá cualquier listado nuevo que se publique a partir del 1 de mayo hasta el 31 de octubre. Los proveedores con listados nuevos publicados durante ese periodo recibirán una factura prorrateada con base en la fecha de entrada en vigor de la lista.

Se facturará una tarifa de lista de aprobación para todos los dispositivos aprobados cuya aprobación esté vigente para todas las aprobaciones existentes al 1 de mayo. No se facturará una tarifa anual de listado a los proveedores por los productos "descontinuados" (EOL) cuyas notificaciones se hayan entregado a PCI por escrito con noventa (90) días de anticipación a la fecha de facturación del 1 de mayo. Un producto descontinuado es un producto que ya no se comercializa para nuevos usos según se describe en la Sección A.13 – Información adicional. Esto solo se aplica a una aprobación completa, y no a artículos individuales dentro de una aprobación. La notificación debe acompañarse con una copia de la notificación de fin de vida útil enviada por el proveedor a sus clientes. Los productos seguirán en la lista de PCI como aprobados hasta la fecha de vencimiento natural de la aprobación con una anotación de que el proveedor dejará de venderlo para nuevos usos, salvo que se requiera el retiro de la aprobación de PCI por otros motivos (p. ej., el riesgo del dispositivo). En cualquier caso, los proveedores no podrán manipular las listas de productos para evitar las tarifas de listado o mantenimiento.

6 Proceso de aprobación

6.1 Convenio de descargo y entrega del informe

Antes de que el laboratorio publique el informe de evaluación, el proveedor deberá firmar un formulario de consentimiento o un convenio de descargo del Acuerdo de Confidencialidad en el que se otorgue permiso para liberar la información al PCI SSC para que considere su aprobación. Además, el proveedor deberá firmar el *Convenio de Descargo del Proveedor de la Industria de Tarjetas de Pago*, que presenta el laboratorio de prueba junto con el informe. Para que se acepte un dispositivo de seguridad de pagos a consideración de aprobación, los laboratorios deben entregar los informes de evaluación del dispositivo de seguridad de pagos **directamente** al PCI SSC.

Antes de que el PCI SSC revise cualquier informe de evaluación para el listado en el sitio web, el proveedor debe entregar una copia firmada del Convenio de Descargo del Proveedor (VRA) en vigor al laboratorio de PTS. La versión en vigor del VRA está disponible en el sitio web público.

Los proveedores y otros terceros que concedan licencias de los productos aprobados de otros proveedores para comercializarlos o distribuirlos con sus propios nombres también deberán firmar un convenio de descargo del proveedor antes de emitir la aprobación.

Las referencias en el convenio de descargo del proveedor a "TPP" o "Producto de Terceros" no se aplican a deltas para aprobaciones que existieron antes de la firma del proveedor del Convenio de descargo del proveedor con tal referencia. Se aplican a todas las aprobaciones nuevas subsiguientes que originen un número nuevo de aprobación y a deltas de las mismas aprobaciones.

En cualquier caso, el Convenio de Descargo del Proveedor, salvo que se reemplace o termine de otra forma conforme a lo previsto en el convenio, solo requerirá una presentación para cubrir todos los productos presentados del proveedor.

6.2 Funciones y responsabilidades

La responsabilidad y facultades del laboratorio se limitan a la aplicación de pruebas de dispositivos de seguridad de pagos y la generación de un informe de evaluación que describa los resultados de las pruebas. Es responsabilidad y facultad del PCI SSC considerar un dispositivo de seguridad de pagos para su aprobación con base en los resultados reportados por el laboratorio.

Es responsabilidad del Laboratorio y del Proveedor conceder un tiempo suficiente a la programación del proyecto: evaluación del dispositivo, presentación del informe para revisión, respuestas a las consultas y reenvío de informes, proceso de aprobación, etc.

6.3 Emisión de la aprobación

El PCI SSC basará su aprobación únicamente en los resultados del informe de evaluación del laboratorio. Todos los informes, consultas de revisores del informe y respuestas del Laboratorio a las consultas se administran a través del portal del PCI SSC. Contra recibo del informe de prueba para una evaluación nueva, el PCI SSC tiene dos semanas (14 días naturales) a partir de que reciba dicho informe para identificar cualquier problema técnico o cuestión que deba resolver el laboratorio de pruebas. Si los revisores consideran que el informe es suficientemente deficiente en calidad, será rechazado antes de que se revise en su totalidad y el laboratorio deberá volver a elaborarlo y presentarlo de nuevo para reiniciar el proceso completo.

Si no se identifican problemas o preguntas para el laboratorio dentro de este plazo, el PCI SSC publicará la información de aprobación en el sitio web y emitirá una carta de aprobación. Si se identifican preguntas o problemas y se envían al laboratorio, el ciclo se reinicia a una semana (siete días naturales) después de que se reciba una respuesta completa y aceptable del laboratorio. El reinicio de siete días no ocurre hasta que se reciba una respuesta aceptable para el último artículo abierto que se haya identificado antes. En caso de que surjan dudas o problemas adicionales, el ciclo se repite hasta que se reciba una respuesta satisfactoria, momento en el cual, el PCI SSC publicará la información en su sitio web y emitirá la carta de aprobación. En cualquier caso, cuando se requiera volver a presentar los informes como parte del proceso para resolver problemas técnicos o dudas, los cambios a cualquier informe subsiguiente al informe inicial deberán hacer utilizando las marcas de revisión, es decir, "tachados".

Los problemas o preguntas adicionales que surjan después del periodo inicial de 14 días se limitan a la misma área de seguridad para las que se generaron los problemas técnicos o preguntas originalmente. En general, esto significa que se limitan a los mismos requisitos de seguridad; sin embargo, la información proporcionada por el laboratorio de pruebas puede afectar otros requisitos de seguridad, que, por lo tanto, estarían dentro de su alcance.

El ciclo (p. ej., un lapso inicial de 14 días naturales) es el mismo para los informes sobre modificaciones a dispositivos aprobados existentes, denominadas cartas o informes "delta", y el PCI SSC publicará la información revisada en el sitio web y emitirá una carta revisada de aprobación salvo que los problemas o preguntas surjan de una manera similar a la arriba mencionada. Los informes de deltas se elaboran utilizando los requisitos principales con los que se evaluó el dispositivo de seguridad de pagos cuando recién se aprobó. Siempre que sea factible, los cambios atribuidos a las deltas usarán marcas de revisión en el informe original. Si no es factible —p. ej. porque existen varias deltas en el mismo dispositivo—, entonces los cambios deben anotarse en forma explícita.

En cualquier caso, las cartas de aprobación podrán emitirse antes si todas las marcas de pago lo aprueban.

La carta de aprobación de PCI y el listado en www.pcisecuritystandards.org contendrán, como mínimo, la siguiente información. Cada característica que se detalla en el Apéndice A "Listado de Dispositivos en el sitio web del PCI SSC*".*

- Identificador del dispositivo de seguridad de pagos
- Número de aprobación
- Tipo de producto
- Clase de aprobación
- Versión
- Fecha de vencimiento
- Soporte de PIN (en línea, sin conexión) – solo para POI
- Administración de claves – solo para POI
- Control de mensajes
- Funciones proporcionadas
- Componentes aprobados

***Nota**:*
El PCI SSC no otorgará ninguna "aprobación parcial" con base en la capacidad de un dispositivo de PTS de cumplir con algunos de los requisitos, pero no todos, de seguridad física o lógica.

Por varios motivos, incluyendo la revocación de aprobación, la información en las cartas de aprobación puede volverse inexacta. Por lo tanto, el sitio web de PCI se considera la fuente acreditada y siempre debe utilizarse para validar el estado de aprobación del producto de un proveedor.

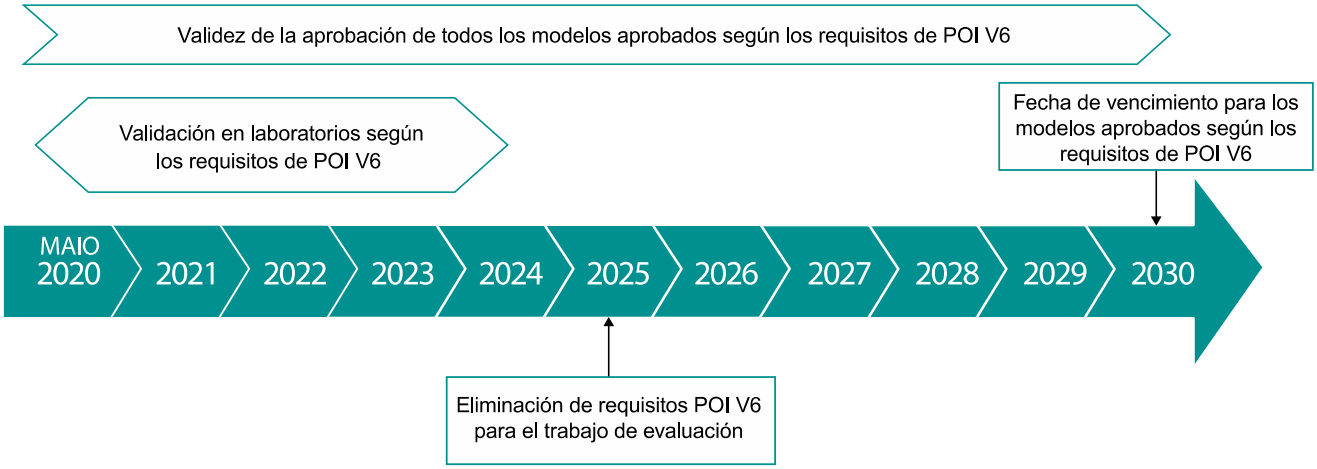
6.4 Retraso de la lista

Los proveedores pueden decidir si retrasan el listado de un dispositivo recién aprobado hasta seis meses como máximo. La notificación por escrito al PCI SSC deberá presentarse a través del laboratorio aplicable junto con el informe de evaluación. Además, el laboratorio debe anotar en la sección de "Notas" del portal de informes de laboratorio la indicación del periodo durante el cual se debe retener el listado del dispositivo.

6.5 Vencimiento de la aprobación

Para mantener la aprobación de un modelo aprobado dado, el proveedor debe hacer que se vuelva a evaluar el modelo del dispositivo aprobado conforme a la versión actual de la norma PCI PTS antes de la fecha de vencimiento, según se muestra en la lista de aprobación de PTS de PCI. Una vez concluida en forma correcta, la aprobación nueva se emitirá conforme a la versión principal aplicable de los requisitos.

El siguiente diagrama muestra la relación entre el vencimiento del modelo de dispositivo probado conforme a la Versión 6 de los requisitos de seguridad de PTS de POI de PCI y su prueba de laboratorio.



Para los dispositivos que incorporan otros dispositivos aprobados por PCI y que, por lo tanto, basan su seguridad en estos subcomponentes (incluso de manera parcial), la fecha de vencimiento será la que ocurra primero entre las evaluaciones, incluyendo el mismo dispositivo incorporado.

7 Cambios a un dispositivo de PTS previamente aprobado

Si un dispositivo de seguridad de pagos aprobado ha sufrido cambios que puedan afectar potencialmente la seguridad, y/o si el proveedor desea que se revise la información de su *Carta de aprobación de POI* o *Carta de aprobación de HSM* y en el sitio web de PCI, el proveedor debe presentar la documentación de cambio adecuada al laboratorio para que se determine si se requiere una evaluación completa. El laboratorio comunicará al PCI SSC cualquier información sobre los cambios a un dispositivo de seguridad de pagos aprobado con anterioridad. Entonces, el PCI SSC indicará las actualizaciones que correspondan en su *Carta de aprobación* revisada y en el sitio web del PCI SSC: www.pcisecuritystandards.org.

Nota:

Si los proveedores de dispositivos de seguridad de pagos pueden dividir la funcionalidad del dispositivo de seguridad de pagos en módulos, ayudaría a minimizar las reevaluaciones debido a que los cambios en el hardware no tendrían impacto en la seguridad del dispositivo de seguridad de pagos.

7.1 Mantenimiento de la aprobación

1. **No se requieren pruebas nuevas para mantener la aprobación si no hay impacto en los requisitos de seguridad**

   Si se revisa el hardware o firmware (incluyendo el software que tiene impacto en la seguridad) del dispositivo de seguridad de pagos aprobado con anterioridad, pero la revisión se considera menor y no tiene impacto negativo en la seguridad, entonces la documentación del cambio se presentará al laboratorio para su revisión. Se recomienda ampliamente que el proveedor utilice el mismo laboratorio que utilizó para la evaluación original.

   Cuando sea adecuado, el laboratorio emitirá una carta al PCI SSC donde describa la naturaleza del cambio, estableciendo que no tiene impacto en el cumplimiento del POI o HSM con los requisitos de seguridad de PCI. Entonces, el PCI SSC revisará la carta para determinar si el cambio tiene algún impacto en el estado de aprobación del dispositivo de seguridad de pagos.

   Suponiendo que no hay impacto, el número de versión nuevo del hardware y/o firmware se considerará "Aprobado" y:

   - Se actualizará la lista del dispositivo de seguridad de pagos aprobado en el sitio web de PCI según corresponda con la información nueva.
   - Se emitirá una carta de aprobación revisada a favor del proveedor.

2. **Se requiere una prueba nueva para mantener la aprobación en caso de un impacto potencial en los requisitos de seguridad**

   Si los cambios al dispositivo tienen un impacto en los requisitos de seguridad del dispositivo de seguridad de pagos, el dispositivo debe someterse a otra evaluación de seguridad. Entonces, el laboratorio presentará un informe nuevo de evaluación al PCI SSC para que considere nuevamente su aprobación. En esta situación, el proveedor debe presentar primero la documentación del cambio al laboratorio, donde se determinará si la naturaleza del cambio tiene un impacto en la seguridad del dispositivo de seguridad de pagos conforme a los requisitos de seguridad vigentes de PCI para dispositivos de seguridad de pagos.

7.2 Límite de la aprobación

El límite de aprobación para trasladar una aprobación de un modelo existente de un dispositivo de seguridad de pagos a un modelo nuevo (o similar) del dispositivo de seguridad de pagos puede alcanzarse de la siguiente manera:

1. El proveedor describe el diseño del modelo nuevo (o similar) del dispositivo de seguridad de pagos en la forma de un documento de revisión de producto.
2. El proveedor envía la documentación al laboratorio seleccionado para su revisión.
3. El laboratorio revisa la documentación (y posiblemente las muestras del dispositivo de seguridad de pagos).
4. El laboratorio trata el proceso de revisión de documentos como una revisión de producto de un dispositivo de seguridad de pagos aprobado existente.
5. Entonces, el laboratorio envía una carta al proveedor para informarle si se requiere o no una evaluación completa.

7.3 Dispositivos compuestos

Los dispositivos compuestos, como las terminales de pago desatendidas, puede evaluarse como parte de una sola evaluación de todos los componentes aplicables o pueden evaluarse con uno o más componentes OEM aprobados con anterioridad. Cuando un dispositivo compuesto incorpora componentes aprobados con anterioridad, deben hacerse las siguientes consideraciones para la evaluación:

- Los informes de evaluación UPT que contienen componentes OEM aprobados por separado deben contener, como mínimo, una tabla resumen de todos los requisitos (ya sea Sí o N/A) de cada módulo que sea pertinente para el factor de forma final del UPT. Esta tabla puede hacer referencia al componente OEM pertinente para cumplimiento con algún requisito específico.
- Todos los requisitos afectados (p. ej. mecanismos adicionales de ingreso de titular de la tarjeta, pantallas, controladores, etc.) por el factor de forma final del UPT deben tratarse a detalle en cada requisito afectado.
- Cuando el laboratorio que evalúa el factor de forma final no es el mismo laboratorio que el laboratorio que evaluó los componentes OEM , el laboratorio debe tener acceso a los informes de laboratorio del componente OEM. Si esos informes no están disponibles, p. ej., porque los proveedores solicitantes son diferentes o por alguna otra restricción, entonces el laboratorio debe determinar la medida de trabajo adicional que se requiere.
- Si el laboratorio no puede confiar, cuando sea necesario, en la información que está disponible en los informes pero no lo está para el laboratorio, y este último no puede llevar a cabo el grado de trabajo adicional necesario para lograr tal confianza, entonces debe rechazar el encargo.
- En cualquier caso, el PCI SSC debe rechazar el informe si, a su juicio, el informe no contiene información adecuada para sustanciar las conclusiones de cumplimiento con los criterios generales de UPT.

Solo se permite el uso de los componentes OEM aprobados conforme a los requisitos de seguridad anteriores para obtener una evaluación de aprobación general UPT sin pruebas adicionales de tales componentes si solo se trata de una versión principal anterior de requisitos. Por ejemplo, puede utilizar los EPP evaluados y aprobados con PCI POI v5.x sin pruebas adicionales de requisitos que cumplieron en forma previa como arte de una evaluación general POI v6. Sin embargo, EPP que se evaluaron y aprobaron con PCI EPP v4.x deben someterse a una evaluación completa conforme a todos los requisitos aplicables de POI v6.

Los requisitos adicionales de seguridad individual en POI v6 que no se evaluaron de manera previa todavía se aplicarán, si es el caso, a la evaluación general UPT. Asimismo, para los dispositivos que incorporan otros dispositivos aprobados por PCI y que, por lo tanto, basan su seguridad en estos subcomponentes (incluso de manera parcial), la fecha de vencimiento será la que ocurra primero entre las fechas de vencimiento de las evaluaciones, incluyendo el mismo dispositivo incorporado.

7.4 Cambios de marca y licencias

No se requiere que los proveedores y otros terceros que concedan licencias de los productos aprobados de otros proveedores para comercializarlos o distribuirlos con sus propios nombres paguen una tarifa de evaluación nueva si el único cambio es en la identificación. Si se realizan cambios al firmware u otro hardware que requieran que un laboratorio de pruebas reconocido por PCI evalúe el posible impacto a la seguridad ocasionado por los cambios, el licenciatario deberá pagar la tarifa de la evaluación nueva. En cualquier caso, el dispositivo con licencia recibirá un número nuevo de aprobación, y la tarifa de listado anual por cada una de dichas aprobaciones se facturará al proveedor del licenciatario o al tercero.

Estas son otras consideraciones adicionales para que un tercero obtenga una licencia de un producto aprobado de un proveedor con la que el tercero desea distribuirlo como su propio producto:

1. El proveedor licenciatario no puede hacer la solicitud en forma directa. El proveedor licenciante debe hacer la solicitud en su representación.

2. El PCI SSC debe recibir todas las solicitudes como una carta de deltas de uno de los laboratorios de PTS reconocidos por el PCI SSC. Si el único cambio es a la identificación del producto, no se cobrará una tarifa nueva de evaluación, pero sí la tarifa de listado anual, como se mencionó anteriormente.

3. No existe ningún requisito para que la versión del producto del licenciatario haga referencia o liste al proveedor original.

4. Los productos pueden tener licencia de otro proveedor incluso si la versión de los requisitos de seguridad con la que se aprobó el producto original ya se retiró de uso para evaluaciones nuevas, siempre y cuando la aprobación no haya vencido aún.

5. Como se mencionó, los productos con licencia que requieran cambios físicos y/o lógicos incurrirán en una tarifa nueva de evaluación. Sin embargo, siempre que el proveedor original siga fabricando el dispositivo a nombre del proveedor licenciatario, el producto con licencia puede evaluarse con la versión de requisitos de seguridad con la se evaluó y aprobó el producto original, incluso si tales requisitos vencieron para aprobaciones nuevas.

6. Si el proveedor licenciatario desea fabricar directamente el producto con licencia o pide a un tercero, que no sea el proveedor original, que fabrique el producto con licencia a su nombre, el producto debe volver a evaluarse como una evaluación nueva conforme a la versión actual de los requisitos de seguridad, salvo que el proveedor licenciante pueda demostrar que conserva los derechos de propiedad intelectual y el control de la ingeniería del mismo. Lo anterior se debe al potencial de cambios en plásticos, etc., que pudieran afectar la seguridad del dispositivo.

Los proveedores que buscan varias aprobaciones para sus propios productos están sujetos a las mismas condiciones para los elementos 2, 3, 4 y 5, según corresponda.

Los proveedores también pueden fabricar dispositivos que solo otros proveedores vayan a vender y/o fabricar. Estos dispositivos pueden evaluarse y listarse aunque el proveedor original nunca pueda vender estos dispositivos en forma directa. Estos dispositivos pueden evaluarse y listarse siempre y cuando se cumplan los siguientes criterios:

- El dispositivo debe ser totalmente capaz de realizar sus funciones previstas para la clase de aprobación conforme a la que se evalúa y puede venderse como un producto completamente funcional. Esto no impide que el dispositivo necesite software adicional, como aplicaciones de pago, pero el firmware del dispositivo debe cumplir con todos los requisitos aplicables.
- El dispositivo debe tener su propia evaluación y listado de producto.
- Cada proveedor segundo que utilice el diseño del dispositivo y/o fabrique el dispositivo debe contar con su propia evaluación completa (NO DE DELTAS) y un listado separado.

No se permitirá la evaluación de dispositivos que requieran hardware y/o firmware adicional para funcionar (tal como componentes individuales). Esos componentes deben integrarse al diseño del dispositivo que cumpla con los requisitos PTS (HSM o POI).

7.5 Retiro de la aprobación

Los proveedores podrán presentar una solicitud por escrito para que el PCI SSC retire una aprobación cuando el proveedor nunca ha vendido ni utilizado ningún dispositivo de un modelo específico aprobado con anterioridad. Esto solo se aplica a una aprobación completa, y no a artículos individuales dentro de una aprobación. La solicitud debe hacerse utilizando el formulario de solicitud de cambio administrativo PTS a través de uno de los laboratorios de prueba reconocidos por PCI. Este formulario está disponible a través de los laboratorios o del Gerente del Programa PTS: pcipts@pcisecuritystandards.org.

7.6 Cambios administrativos

Los proveedores que hayan tenido algún cambio de nombre legal y deseen actualizar sus listados de aprobación como corresponda, deberán presentar un formulario de solicitud de cambio administrativo PTS a través de un laboratorio de pruebas PTS reconocido. El proveedor también deberá presentar un nuevo convenio de descargo de proveedor con la nueva razón social. Si la apariencia del dispositivo cambia para reflejar el nombre nuevo (etiquetas o identificación), deberá emitirse un informe delta a través de uno de los laboratorios.

Los proveedores que deseen cambiar el nombre del modelo de un dispositivo aprobado también deberán usar el formulario de solicitud de cambio administrativo PTS. Sin embargo, si se ha vendido algún dispositivo con el nombre del modelo anterior, deberán listarse ambos nombres. Además, debe crearse una política nueva de seguridad, y debe hacer referencia a los nombres anteriores y los nuevos o bien listarla en paralelo a la política existente. Asimismo, las imágenes del dispositivo utilizadas en el sitio web www.pcisecuritystandards.orgdeberán incluir los modelos anteriores y los nuevos.

8 Notificación después de una vulneración o riesgo de seguridad

Los proveedores deben notificar al PCI SSC sobre cualquier vulneración o riesgo de seguridad que ocurra en relación con un dispositivo de seguridad de pagos aprobado utilizando los procedimientos descritos en esta sección.

8.1 Notificación y tiempos

Independientemente de cualquier otra obligación legal que el proveedor pudiese tener, el proveedor deberá notificar de inmediato al PCI Security Standards Council (el "Consejo") sobre cualquier vulneración o riesgo de seguridad en relación con cualquiera de lo siguiente:

- Módulo de seguridad del punto de interacción o hardware.
- Instalación de generación de claves.
- Instalación de carga de claves.

El proveedor también deberá proporcionar retroalimentación inmediata sobre cualquier impacto (actual o potencial) que esta vulneración haya tenido o pueda tener.

Nota:

La notificación deberá efectuarse a más tardar 24 horas después de que el proveedor se entere de la vulneración o riesgo de seguridad.

8.2 Formulario de notificación

La notificación inicial del proveedor respecto a la vulneración o riesgo de seguridad deberá hacerse por medio de una llamada telefónica al PCI SSC al +1-781-876-8855 (opción #3, seleccionando "Programa PIN"), seguida de un correo electrónico (pcipts@pcisecuritystandards.org) en el que se proporcionen todos los detalles de la vulneración o riesgo de seguridad.

8.3 Detalles de la notificación

Después de la notificación de una vulneración o riesgo de seguridad, el proveedor deberá entregar al PCI SSC toda la información pertinente respecto a la vulneración o riesgo de seguridad. Lo anterior incluye, entre otras cosas:

- El número y ubicación de los productos reales afectados.
- El número de cuentas en riesgo (si se sabe).
- Datos sobre cualquier clave en riesgo.
- Cualquier informe que detalle la vulneración o riesgo de seguridad.
- Cualquier informe o evaluación realizados para investigar la vulneración o riesgo de seguridad.

El PCI SSC, según lo convenido conforme a los términos del *Convenio de descargo del proveedor de la Industria de tarjetas de pago,* podrá compartir esta información con los laboratorios reconocidos por PCI para que se evalúe la vulneración o riesgo de seguridad para mitigar o evitar cualquier vulneración o riesgo de seguridad futuros. Como resultado de esta notificación, el PCI SSC trabajará con el proveedor para corregir cualquier debilidad de seguridad y elaborará un documento de orientación para los clientes de ese proveedor, informándoles sobre cualquier posible vulnerabilidad y detallando las acciones que deben tomarse para mitigar o evitar cualquier vulneración o riesgo de seguridad futuros.

8.4 Acciones después de una vulneración o riesgo de seguridad

En caso de que se haya notificado al PCI SSC sobre una debilidad de seguridad o un riesgo real en relación con un producto en específico o un grupo de productos aprobados, el PCI SSC tomará las siguientes medidas:

- Notificará a los participantes de las marcas de pago de PCI que ha ocurrido una debilidad o riesgo de seguridad.
- Intentará obtener la terminal en riesgo para evaluar la manera exacta en la que ocurrió el riesgo. Lo anterior puede incluir el uso de laboratorios reconocidos por PCI.
- Se comunicará con el proveedor para informarle que su producto tiene una debilidad de seguridad o está en riesgo y, cuando sea posible, compartirá la información relacionada con la debilidad o riesgo reales.
- Trabajará con el proveedor para intentar mitigar o evitar mayores riesgos.
- Trabajará con las dependencias del orden público adecuadas para ayudar a mitigar o evitar riesgos futuros.
- Evaluará el producto en riesgo, ya sea de manera interna o conforme a los términos del *Convenio de descargo del proveedor de la Industria de tarjetas de pago* del PCI SSC, por medio de los laboratorios reconocidos por PCI para identificar la causa del riesgo.

8.5 Retiro de la aprobación

El PCI SSC se reserva el derecho de retirar la aprobación de un dispositivo POI o HSM y, en consecuencia, actualizar la *Lista de dispositivos de PTS aprobados por PCI.* Algunos de los motivos para retirar la aprobación son:

- Cuando es claro que el dispositivo de seguridad de pagos no ofrece protección suficiente contra amenazas actuales y no cumple con los requisitos de seguridad. Si el PCI SSC considera que el dispositivo de seguridad de pagos tiene una debilidad de seguridad o está un riesgo, el PCI SSC notificará al proveedor por escrito sobre su intención de retirar la aprobación del dispositivo de seguridad de pagos.
- Cuando el proveedor no cumple con las obligaciones contractuales con el PCI SSC o no sigue en forma estricta los términos de participación en el programa PCI PTS según se describen en este documento o el *Convenio de descargo del proveedor de la Industria de tarjetas de pago.*

9 Términos y condiciones legales

La aprobación del PCI SSC se aplica solo a los dispositivos de seguridad de pagos que sean idénticos al dispositivo de seguridad de pagos probado por un laboratorio reconocido por el PCI Security Standards Council. Si algún aspecto del dispositivo de seguridad de pagos es diferente del dispositivo probado por el laboratorio, incluso si el dispositivo de seguridad de pagos cumple con la descripción básica del producto contenida en la carta de aprobación, entonces el modelo del dispositivo de seguridad de pagos no se considerará aprobado, ni se promoverá como aprobado. Por ejemplo, si un dispositivo de seguridad de pagos contiene firmware, software o construcción física que tiene el mismo nombre o número de modelo que los probados por el laboratorio, pero, de hecho, no es idéntico a las muestras del dispositivo de seguridad de pagos probadas en el laboratorio, entonces, el dispositivo de seguridad de pagos no se considerará ni se promoverá como aprobado.

Ningún proveedor o tercero podrá referirse a un dispositivo de seguridad de pagos como "Aprobado por PCI" ni declarar de otra manera ni implicar que el PCI SSC ha aprobado parcial o totalmente algún aspecto de un proveedor o sus dispositivos de seguridad de pagos, salvo en la medida y sujeto a los términos y restricciones estipulados en forma expresa en un contrato con el PCI SSC o en una carta de aprobación. El PCI SSC prohíbe en forma estricta y activa todas las demás referencias a la aprobación del PCI SSC.

Cuando el PCI SSC otorgue una aprobación, lo hará para asegurar ciertas características de seguridad y operativas importantes para cumplir con los objetivos del PCI SSC, pero la aprobación no incluye, bajo ninguna circunstancia, ningún respaldo o garantía respecto a la funcionalidad, calidad o desempeño de algún producto o servicio en particular. El PCI SSC no garantiza ningún producto o servicio proporcionado por terceros. La aprobación no incluye ni implica, bajo ninguna circunstancia, garantías del PCI SSC respecto a algún producto, incluyendo, entre otras, garantías implícitas de comerciabilidad, adecuación para un fin o no infracción, las cuales quedan excluidas en forma expresa por el PCI SSC. Todos los derechos y recursos respecto a los productos y servicios que hayan recibido una aprobación serán estipulados por la parte que proporciona tales productos o servicios, y no por el PCI SSC ni por los participantes de las marcas de pago.

10 Glosario de términos y acrónimos

Término	Definición
Clase de aprobación	La clase de aprobación describe los requisitos de evaluación con los que se probó el dispositivo aprobado. Véase el Apéndice A.
COTS	Dispositivo estándar comercial. Dispositivo móvil (p. ej., teléfono inteligente o tableta) para distribución masiva no destinado específicamente al procesamiento de pagos.
CTLS	Sin contacto.
Dispositivo	Dispositivo de pago; puede ser parte de una terminal.
EPP	Ensamblador de cifrado de PIN; clase de aprobación, designación de los dispositivos integrables (OEM) que se integrarán a la terminal operada por el titular de la tarjeta. Véase el Apéndice A.
Marco de evaluación	Conjunto de requisitos para los proveedores, metodología de prueba para los laboratorios, proceso de aprobación para los productos y lista de aprobación pertenecientes a un tipo dado de dispositivo de seguridad de pagos (dispositivo POI, HSM).
HSM	Módulo de seguridad de hardware; clase de aprobación dirigida a los dispositivos que admiten varios procesamientos de pago, y aplicaciones y procesos de autenticación de titulares de tarjetas. Véase el Apéndice A.
Lector híbrido	Un dispositivo que incorpora capacidades de captura de datos de tarjetas, ya sea de una tarjeta con banda magnética o de una tarjeta con circuito integrado (también conocida como tarjeta inteligente o tarjeta con chip).
ICCR	Lector de tarjetas con circuito integrado
KLD	Dispositivo de carga de claves.
MSR	Lector de banda magnética.
OEM	Fabricante del equipo original.
Dispositivo de seguridad de pagos	Un dispositivo completo (por ejemplo, un dispositivo de aceptación de PIN orientado al consumidor o un HSM) cuyas características contribuyen a la seguridad de los pagos electrónicos minoristas u otras transacciones financieras.
Programa de evaluación de seguridad de dispositivos de PTS de PCI	El marco de evaluación del PCI SSC para los dispositivos del sistema de pagos.

Término	Definición
PED	Dispositivo con entrada de PIN; clase de aprobación dirigida a dispositivos con entrada de PIN y capacidad de procesamiento de PIN, ya sea asistida o no asistida, cuyo propósito principal es capturar y transmitir el PIN a un lector ICC y/o a otro dispositivo de procesamiento, tal como un sistema host. Un dispositivo con entrada de PIN (PED) debe tener pantalla integrada, a menos que sea específico para entrada de PIN. Véase el Apéndice A.
POI	Punto de interacción.
Dispositivo POI	Dispositivo utilizado en el punto de interacción con un consumidor.
Tipo de producto	El tipo de producto describe tanto la clase de aprobación de un dispositivo y si el dispositivo es un módulo que se integrará (OEM) o no.
PTS	Seguridad de transacciones con PIN, el marco del PCI SSC para los dispositivos de seguridad de pagos. Se refiere a los dispositivos POI y HSM, de manera conjunta.
Dispositivos de PTS	Dispositivos de seguridad de pagos, dispositivos POI y HSM.
PTS-HSM	El submarco del marco de seguridad de dispositivos de PTS de PCI que trata la seguridad de HSM.
PTS-POI	El submarco del marco de seguridad de dispositivos de PTS de PCI que trata la seguridad de los dispositivos frente al consumidor.
RAP	Plataforma de administración remota para HSM.
SCR	Clase de aprobación del lector de tarjetas seguro.
SCRP	Clase de aprobación del PIN del lector de tarjetas seguro.
SPoC	Entrada de PIN basada en software en COTS.
SRED	Lectura segura e intercambio seguro de datos
Terminal	Dispositivo comercial con una función empresarial. Puede dedicarse a un pago (terminal POS con ensamblador de PIN integrado o separado) o dispensador de producto (por ejemplo, un cajero automático o autoservicio en gasolineras).
Ciclo de pruebas	Conclusión de todos los procedimientos de pruebas realizados a una sola versión del dispositivo de seguridad de pagos del proveedor.
UPT	Terminal de pago no asistida; clase de aprobación que designa los dispositivos de pago operados por el titular de la tarjeta (autoservicio) que lee, captura y transmite información de la tarjeta en conjunto con un dispositivo de autoservicio no asistido. Véase el Apéndice A.

Apéndice A: Listado de dispositivos en el sitio web del PCI SSC

A continuación se enumeran las características de un listado de dispositivos en el sitio web del PCI SSC.

A.1 Punto de Interacción (POI)

Para lo fines de estos requisitos, un **dispositivo POI con aceptación de PIN** se define como:

> *Un dispositivo que permite la entrada de PIN, utilizado para comprar bienes o servicios o entregar dinero en efectivo. Un POI aprobado ha cumplido con todos los requisitos de PTS de POI de PCI aplicables para la entrada de PIN en línea y/o sin conexión, y ha definido con claridad el límite físico y lógico para todas las funciones relacionadas con la entrada de PIN.*

Además, los dispositivos POI que no aceptan PIN pueden validarse y aprobarse si cumplen con los requisitos de Lectura e intercambio seguros de datos (SRED) y, si corresponde, a los requisitos de protocolos abiertos. Estos dispositivos debe anotarse en forma explícita como no aprobados para aceptación de PIN.

Los lectores de tarjetas seguras y los lectores de tarjetas seguras con PIN deben validarse con los requisitos descritos en el *Apéndice B: Aplicabilidad de los requisitos* de los *Requisitos de seguridad modular del punto de interacción (POI) para la seguridad de transacciones con PIN (PTS).*

Todas las clases de aprobación están sujetas a los requisitos de seguridad de ciclo de vida.

Un dispositivo POI puede ser independiente y no integrable, en cuyo caso podrá aplicarse la clase de aprobación PED. Esta clase puede aplicarse a dispositivos atendidos y desatendidos. Sin embargo, los proveedores pueden decidir listar una terminal no atendida según la clase UPT si cumple los requisitos adecuados.

Si el dispositivo POI está diseñado para integrarse en un conjunto más amplio (p. ej., una máquina expendedora o cajero automático), entonces se aplicaría la clase de aprobación EPP o PED. En cada caso, puede haber otras funcionalidades presentes ademas de la captura y transmisión de PIN (p. ej. pantalla, lector de tarjeta). Los dispositivos que ingresen a esta categoría tendrán la propiedad del tipo de producto con el prefijo de la palabra "OEM" en la página principal del listado para anunciar en forma inequívoca su naturaleza modular.

Los dispositivos POI que combinan la entrega de bienes (p. ej. gasolina) o servicios (máquina de venta de billetes) con pago realizado con PIN son candidatos para la clase de aprobación UPT. Estos POI pueden incluir módulos OEM aprobados.

Los dispositivos POI presentados para pruebas deben identificarse adecuadamente de forma que los clientes de los participantes de PCI o sus agentes puedan estar seguros de adquirir un POI que ha sido aprobado por PCI.

A.2 Módulo de seguridad de hardware (HSM)

Para los fines de estos requisitos, un **HSM**se define como:

> *Dispositivo de hardware protegido física y lógicamente que proporciona un conjunto seguro de servicios criptográficos. Incluye hardware, firmware, software o una combinación de estos que implementa lógica criptográfica, procesos criptográficos o ambos, incluyendo algoritmos criptográficos.*

Asimismo, este documento introduce una estructura de aprobación de dos niveles para HSM. Estos dos niveles se diferencian solo en la sección de requisitos de seguridad física descrita en los *Requisitos de prueba derivados del HSM de PCI.* El HSM puede aprobarse si fue diseñado para usarse en ambientes controlados definidos en *ISO 134912: Banca — Dispositivos criptográficos seguros (minoristas)* o aprobados para su uso en cualquier entorno operativo. Estas categorías son:

- **Restringida:** La aprobación es válida solo cuando se implementa en entornos controlados o más robustos (p. ej., entornos seguros), como se define en la norma ISO 13491-2 y en la Política de seguridad de HSM de PCI del dispositivo.
- **No restringida:** La aprobación es válida en cualquier entorno.

A.3 Dispositivos con aprobación vencida

Estos son dispositivos cuya aprobación ha vencido, como se indica en la sección “Fecha de vencimiento” de este documento. Para obtener información específica relacionada con el uso de marcas de pago en dispositivos vencidos, comuníquese con las marcas de pago de interés.

A.4 Identificador del dispositivo

PCI utiliza el identificador de dispositivo para señalar toda la información pertinente representativa de un punto de interacción (POI) o módulo de seguridad de hardware aprobado (HSM), y consiste en:

- Nombre del proveedor
- Nombre y número del modelo
- Número de hardware
- Número de firmware
- Número de aplicación, si corresponde

El nombre y número del modelo deben ser visibles y distinguirse en el dispositivo, y no ser parte de una cadena de caracteres más larga. El dispositivo debe mostrar los números de versión del hardware y del firmware de acuerdo con la aprobación del dispositivo, reflejando información de la lista de dispositivos aprobados en la página web pública de PCI. El número del hardware debe aparecer en una etiqueta adherida al dispositivo y distinguirse claramente como la versión de hardware, p. ej., número de HW, HWID, etc. El número de versión del firmware y de la aplicación y, opcionalmente el del hardware, deben aparecer en la pantalla o imprimirse durante el arranque del sistema o a solicitud. Esto incluye todos los requisitos de seguridad que se abordan en las pruebas, incluyendo los protocolos SRED y abiertos. Si la etiqueta que indica la versión de hardware no queda a la vista al instalar el dispositivo, tal como en el ensamblador de cifrado de PIN (EPP) en un cajero automático, deben existir otros medios para mostrar el número de versión. Esto deberá ilustrarse con fotografías proporcionadas en el informe de evaluación.

Para garantizar que el dispositivo de seguridad de pago fue aprobado, se recomienda enfáticamente a los clientes adquirentes o sus representantes comprar e implementar solo los modelos de dispositivos cuya información coincida exactamente con las designaciones proporcionadas en los componentes de los identificadores del los dispositivos POI o del HSM.

Cuadro 3: Ejemplo de un identificador del dispositivo (cinco componentes)

Componente	Descripción
Nombre del proveedor	Acme
Nombre y número del modelo del POI	Ensamblador de PIN 600
Número de hardware	NN-421-000-AB
Número de firmware	Versión 1.01
Número de aplicación	PCI 4.53

El identificador del dispositivo se incluirá en la carta de aprobación y en el sitio web de PCI. Si se utiliza un dispositivo de seguridad de pago idéntico en toda una familia de dispositivos, se advierte a los proveedores que no deben usar un número de hardware (ver a continuación) que pueda restringir la aprobación a solo ese modelo de dispositivo específicamente.

A.5 Nombre y número del módulo

El nombre y número del modelo no pueden contener caracteres variables. Todos los dispositivos dentro de una familia de dispositivos que se pretenda comercializar con el mismo número de aprobación deben nombrarse explícitamente, así como presentarse fotografías de los dispositivos en cuestión para que aparezcan tanto en el informe de evaluación como en la lista de dispositivos aprobados. El proveedor no puede usar un nombre de modelo idéntico para más de un dispositivo aprobado en virtud de la publicación de una versión principal de los requisitos de seguridad.

A.6 Número de hardware

Número de hardware representa el conjunto de componentes del hardware específico utilizado en el dispositivo de seguridad de pago aprobado. Los campos que lo conforman pueden consistir en una combinación de caracteres alfanuméricos fijos y variables. No se permiten caracteres variables para características físicas o lógicas del dispositivo que afecten la seguridad; estas deben denotarse con caracteres fijos. El uso de caracteres variables deberá validarlo el laboratorio de pruebas a fin de no comprometer la seguridad.

Nota:

El número de versión del firmware también puede estar sujeto al uso de variables de manera congruente con la de los números de versión del hardware.

PCI designa todos los campos variables con una "x". La “x” representa campos en el número de hardware que el proveedor puede cambiar en cualquier momento para denotar la configuración de un dispositivo diferente. Por ejemplo: código de uso del país, código del cliente, interfaz de comunicación, color del dispositivo, etc.

Los campos con "x" han sido evaluados por el laboratorio y el PCI SSC para no afectar los requisitos de seguridad del POI o del HSM o la aprobación del proveedor. Para garantizar que el dispositivo de seguridad de pago se ha autorizado, se recomienda enfáticamente que los clientes adquirentes o sus representantes compren e implementen solo aquellos dispositivos cuyos caracteres alfanuméricos fijos coincidan exactamente con el número de hardware que aparece en la Lista de dispositivos de Seguridad de la transacción con PIN (PTS) aprobados por PCI.

Nota:

Es posible que los proveedores hayan producido dispositivos de seguridad de pago con el mismo nombre y numero de modelo (antes de que el laboratorio validara el cumplimiento normativo) que no satisfacen los requisitos de seguridad de estos dispositivos.

Las opciones que no pueden ser caracteres variables incluyen aquellas que conciernen directamente al cumplimiento de los requisitos de seguridad. Por ejemplo, existen requisitos para los lectores de banda magnética (MSR) y los lectores de tarjetas de circuito integrado (ICCR). Los caracteres variables no pueden utilizarse para indicar si un dispositivo contiene un MSR o un ICCR. Existe el requisito de disponer elementos que eviten la observación de los valores del PIN que ingresa un titular de tarjeta; dicho requisito se puede cumplir con protectores de privacidad o con el entorno instalado del dispositivo o bien, una combinación de ambos. No es apropiado utilizar variables comodín en las opciones si el dispositivo cuenta con más de un mecanismo para impedir la observación.

Si el dispositivo es compatible con los protocolos SRED y abiertos, no se permitirían algunas opciones que normalmente serían aceptables para ser identificadas por una variable comodín. Por ejemplo, la adición de lectores sin contacto o la inclusión de diferentes paquetes de comunicación. En estos casos, las configuraciones específicas validadas por el laboratorio reconocido de PTS deben destacarse de manera explícita en la aprobación.

Además, todas las variables comodín, pertinentes tanto en el aspecto de seguridad como en otros aspectos, deben definirse claramente, así como documentar las opciones disponibles y su función tanto en el informe de evaluación como en la política de seguridad.

Cuadro 4: Ejemplos de uso de números de hardware

Número de hardware del dispositivo de seguridad de pago en la lista de aprobación	Comentarios
NN-421-000-AB	El hardware número NN-421-000-AB del identificador del dispositivo no emplea la variable "**x**." Por lo tanto, el dispositivo de seguridad de pago que se implementará debe coincidir exactamente con el número de hardware para que el dispositivo de PTS se considere un dispositivo de seguridad de pago aprobado (componente del hardware).
NN-4**x**1-0**x**0-A**x**	El hardware número NN-4**x**1-0**x**0-A**x** del identificador del dispositivo emplea la variable "**x**." Por lo tanto, el dispositivo de seguridad de pago que se implementará debe coincidir exactamente con el número de hardware solo en las posiciones donde no haya una "**x**."
Número real del hardware del POI proporcionado por el proveedor	**Comentarios**
NN-421-090-AC	Si en el sitio web de PCI aparece NN-421-000-AB como el número de hardware en el identificador del dispositivo, entonces el dispositivo de seguridad de pago con el número de hardware NN-421-090-AC **no** puede considerarse un dispositivo aprobado (componente del hardware). Sin embargo, si aparece NN-4**x**1-0**x**0-A**x** como el número de hardware en el identificador del dispositivo, entonces el dispositivo con el número de hardware NN-421-090-AC **puede** considerarse un dispositivo aprobado (componente del hardware).
NN-421-090-YC	Si en el sitio web de PCI aparece NN-4**x**1-0**x**0-A**x** como el número de hardware en el identificador del dispositivo, entonces el dispositivo de seguridad de pago con el número de hardware NN-421-090-YC **no** puede considerarse un dispositivo aprobado (componente del hardware).

A.7 Política de seguridad

El proveedor del dispositivo proporciona a los usuarios una política de seguridad, que aborda el uso adecuado del dispositivo de manera segura, e incluye información sobre responsabilidades de administración de claves, responsabilidades administrativas, la funcionalidad del dispositivo, su identificación y los requisitos del entorno. La política de seguridad debe definir las funciones admitidas por el dispositivo e indicar los servicios disponibles para cada función en un formato tabular determinista. El dispositivo es capaz de realizar solo las funciones previstas, es decir, no hay funcionalidades ocultas. Las únicas funciones que el dispositivo puede realizar son aquellas permitidas por la política.

A.8 Número de aprobación

El PCI SSC asigna los números de aprobación al momento de otorgar la aprobación, y estos permanecerán inalterables durante la vigencia de la aprobación del dispositivo.

A.9 Tipo de producto

El tipo de producto proporciona información tanto sobre la clase de aprobación de un dispositivo como sobre si el dispositivo es un módulo que debe integrarse (OEM), o si es un equipo listo para implementación. El tipo de producto deberá especificar **"OEM"** si el dispositivo aprobado está claramente diseñado para integrarse a un conjunto más amplio, o señalarse como un dispositivo sin entrada de PIN (sin PED) para diferenciar inequívocamente un dispositivo de POI con aceptación de PIN de otro sin aceptación de PIN.

Los proveedores que fabrican productos OEM autónomos, que son módulos complementarios o adicionales —es decir, módulos de PED totalmente funcionales que integran todos los componentes requeridos— para terminales de pago desatendidas (UPT) pueden optar por asociarse con los proveedores de factor de forma final de dichas UPT (p. ej., dispensadores automáticos de combustible (AFD) o kioscos). El producto OEM del proveedor puede cumplir con la mayoría de los requisitos de seguridad generales de las UPT, y el proveedor de OEM puede enviar ese producto junto con información adicional del proveedor de factor de forma final en representación de ese proveedor —tal como el diseño para AFD o kiosco— al laboratorio para su evaluación como una UPT.

El producto OEM del proveedor no puede recibir una aprobación como UPT porque es posible que el producto de factor de forma final real tenga otras interfaces para titulares de tarjeta (p. ej., pantallas o dispositivos para ingresar datos) u otras características dentro del alcance de los requisitos de seguridad de las UPT. El producto de factor de forma final del vendedor recibiría la aprobación como UPT. Al producto OEM del proveedor se le asignaría un número de aprobación distinto y se enumeraría también por separado; además, se le enumeraría como un componente aprobado del producto UPT, de manera similar a la que otros productos OEM se enumeran.

A.10 Clase de aprobación

PCI utiliza la **Clase de aprobación** para garantizar que la aprobación de sus dispositivos de seguridad de pago describa con precisión los cambiantes diseños, arquitecturas e implementaciones actuales. Todos los POI y HSM aprobados por el PCI SSC en el marco del Programa de evaluación de seguridad de los dispositivos de PTS de PCI, independientemente de la Clase de aprobación designada, conllevan un estado de aprobación plena de PCI. Las instituciones financieras, o sus representantes (p. ej., comerciantes o procesadores), deben cerciorarse de comprender las diferentes clases, ya que estas indican la manera en que el dispositivo de seguridad de pago ha cumplido con los requisitos de seguridad de PCI sobre los dispositivos de PTS.

Cuadro 5: Descripciones de las clases de aprobación

Clase de aprobación	Descripción	Posibles características *(consulte el Cuadro 7 a continuación)*
EPP	Clase de aprobación dispuesta para módulos de entrada y cifrado de PIN seguros en un dispositivo con aceptación de PIN desatendido. Un EPP puede tener una pantalla o un lector de tarjetas integrados o depender de pantallas o lectores de tarjetas externos instalados en el dispositivo desatendido. Generalmente, se utiliza en un dispositivo con aceptación de PIN desatendido, y es controlado por un controlador del dispositivo. Tiene límites físicos y lógicos claramente definidos y una carcasa resistente a, o a prueba de, manipulaciones. Como mínimo, un dispositivo que se envía para aprobación EPP debe contar con un teclado y su módulo criptográfico seguro integrado. Los fabricantes de equipos originales (OEM) o los proveedores de ensambladores de cifrado de PIN (EPP) para fabricantes de dispositivos con aceptación de PIN (p. ej., cajeros automáticos o UPT) y otros tipos de dispositivos de autoservicio pueden enviar solo un EPP a laboratorio para su evaluación y aprobación. Como componente integral de un POI totalmente funcional, un EPP OEM aprobado puede utilizarse en otro dispositivo de pago, como un cajero automático o UPT para minimizar la redundancia de las pruebas. No obstante, las UPT que utilicen un EPP aprobado aún deberán someterse a evaluaciones de laboratorio a fin de obtener la aprobación general para la UPT.	Pantalla Soporte de PIN Control de mensajes Administración de clave Tecnología con entrada de PIN ICCR MSR CTLS SRED OP

Clase de aprobación	Descripción	Posibles características *(consulte el Cuadro 7 a continuación)*
HSM	Los HSM pueden admitir diversas aplicaciones y procesos de autenticación de titulares de tarjeta y de procesos de pago. Los procesos importantes para el conjunto de requisitos descritos en este documento son: ▪ Procesamiento de los PIN ▪ Protocolo 3-D Secure ▪ Verificación de tarjetas ▪ Producción y personalización de tarjetas ▪ Tarjeta EFTPOS (transferencia electrónica de fondos en el punto de servicio) ▪ Intercambio en cajeros automáticos ▪ Recarga de tarjeta de efectivo ▪ Integridad de los datos ▪ Procesamiento de transacciones con tarjeta de chip	N/A
KLD	Un dispositivo seguro criptográfico (SCD) que puede utilizarse para recibir, almacenar y transferir datos de manera segura entre equipos criptográficos y de comunicaciones compatibles. Las funciones de transferencia y carga de claves incluyen lo siguiente: ▪ Exportación de una clave desde un SCD a otro SCD en forma de texto simple, componente o cifrada. ▪ Exportación del componente de una clave desde un SCD a un paquete a prueba de manipulación (p. ej. correo con copia oculta). ▪ Importación de componentes de claves a un SCD desde un paquete a prueba de manipulación. Almacenamiento temporal de la clave en forma de texto simple, componente o cifrada dentro de un SCD durante la transferencia.	N/A

Clase de aprobación	Descripción	Posibles características *(consulte el Cuadro 7 a continuación)*
Dispositivo sin entrada de PIN	Clase de aprobación de dispositivos de POI que NO permite la entrada de PIN para transacciones con tarjeta de pago. Aplica a TODOS los dispositivos de POI o combinaciones de dispositivos, atendidos y desatendidos, que no admiten transacciones de pago con PIN. Es posible que los tipos de productos OEM requieran mayor integración en una terminal de POI. El dispositivo o cualquier combinación de hardware se puede utilizar como se juzgue pertinente para funcionar en una red de adquirentes. El firmware debe incluir una aplicación de pago aprobada por el adquirente, necesaria para funcionar. Los dispositivos de POI sin entrada de PIN previstos para uso en un entorno atendido deben ser unidades autónomas completamente funcionales capaces de procesar transacciones de pago, y deben incluir una interfaz del comerciante, necesaria para funcionar. Los dispositivos de POI sin entrada de PIN (terminales) se validan de acuerdo con los requisitos de los protocolos de Lectura e intercambio seguros de datos (SRED) y, si corresponde, abiertos. Estos dispositivos NO están aprobados para aceptación de PIN.	ICCR MSR CTLS SRED OP
PED	Clase de aprobación dispuesta para dispositivos POI, originalmente diseñados para admitir pago con entrada de PIN, y específico para pagos. Un dispositivo con entrada de PIN (PED) debe tener pantalla integrada, a menos que sea específico para entrada de PIN. Esta clase puede abarcar entornos tanto atendidos como desatendidos y productos OEM o independientes.	Pantalla Soporte de PIN Control de mensajes Administración de clave Tecnología con entrada de PIN ICCR MSR CTLS SRED OP
RAP	Esta clase es para plataformas que se utilizan para administrar los HSM de manera remota. Dicha administración puede incluir servicios de configuración de dispositivos y carga de claves.	N/A

Clase de aprobación	Descripción	Posibles características *(consulte el Cuadro 7 a continuación)*
SCR	Un lector de tarjetas de cifrado que: ▪ Esté previsto para usarse con un dispositivo no seguro, tal como un teléfono celular u otro dispositivo; o bien ▪ Se pueda definir como un tipo de producto OEM que deba integrarse en la terminal POI o cajero automático. Los tipos de productos OEM pueden contener una aplicación de pago y ser capaces de usarse independientemente o como un dispositivo secundario para procesar datos de cuentas de manera segura (SRED) y, si corresponde, verificar PIN sin conexión y requerir conexión a un módulo, terminal o ensamblador de PIN seguros. Un lector de tarjetas seguro puede ser: ▪ Híbrido ▪ Solo para tarjetas de banda magnética ▪ Solo para tarjetas con chip ▪ Solo sin contacto Los SCR deben cumplir, según corresponda, con los requisitos para ICCR y/o MSR señalados en el Apéndice B de los *Requisitos de seguridad de PCI sobre PTS en los POI* y los requisitos de SRED. Si el dispositivo es capaz de comunicarse en una red IP o usa un protocolo de dominio público (como Wi-Fi o Bluetooth, entre otros), entonces también deben cumplirse los requisitos especificados en los protocolos abiertos. Aplican otros requisitos, como B1, Autopruebas, y B9, Números aleatorios, dependiendo de la funcionalidad del dispositivo. Si un SCR procesa PIN —es decir, admite autenticación de PIN sin conexión a través de un componente de ICCR o si formatea y cifra un bloqueo de PIN para enviarlo en línea directo al host— debe validarse junto con un dispositivo de entrada de PIN específico (p. ej., PED o EPP) para validar la seguridad de la interacción, incluyendo el establecimiento de la relación de la codificación. El PED debe aprobarse previamente u obtener aprobación simultáneamente con la del SCR en la misma evaluación de laboratorio o en otra evaluación simultánea independiente.	Soporte de PIN ICCR MSR CTLS SRED OP

Clase de aprobación	Descripción	Posibles características *(consulte el Cuadro 7 a continuación)*
SCRP	Lector de tarjetas de cifrado que se pretende utilizar con un dispositivo comercial estándar (COTS), como un teléfono o una tableta. El PIN de un lector de tarjeta seguro (SCRP o SCR-PIN) puede ser: ▪ Un lector de contacto solo de tarjetas con chip. ▪ Un lector sin contacto solo de tarjetas con chip. ▪ Un lector que admita tarjetas de chip tanto de contacto como sin contacto. ▪ Un lector híbrido, que incluye un lector de tarjeta de banda magnética y funcionalidad de tarjeta con chip de contacto y/o sin contacto. Los SCRP deben cumplir, según corresponda, con los requisitos para ICCR señalados en el Apéndice B de los *Requisitos de seguridad de PCI sobre PTS en los POI* y los requisitos de SRED. Si el dispositivo es capaz de comunicarse en una red IP o usa un protocolo de dominio público (como Wi-Fi o Bluetooth, entre otros), entonces también deben cumplirse los requisitos especificados en los protocolos abiertos. Aplican otros requisitos de las secciones Física y Lógica, dependiendo de la funcionalidad del dispositivo. Los SCRP traducen los PIN de los bloqueos de PIN recibidos desde la aplicación de pago en el dispositivo COTS a un bloqueo de PIN, ya sea para ser trasladados al host de procesamiento o para verificar sin conexión la tarjeta con chip de contacto.	Soporte de PIN Administración de clave ICCR MSR CTLS SRED OP
UPT	Esta clase abarca dispositivos de pago operados por los titulares de tarjetas, que leen, capturan y transmiten información de la tarjeta junto con un dispositivo de autoservicio desatendido, incluyendo, entre otras cosas: 1. Dispensadores automáticos de combustible 2. Máquinas expendedoras de boletos 3. Máquinas expendedoras de productos Es posible que las UPT tengan una arquitectura compleja que combina directamente el pago y la entrega de productos o servicios.	Pantalla Soporte de PIN Control de mensajes Administración de clave Tecnología con entrada de PIN ICCR MSR CTLS SRED OP

A.11 Versión

Se refiere a la versión de los requisitos de seguridad que el dispositivo debió cumplir. Cada clase de aprobación debe seguir su propio calendario de lanzamiento de versiones.

A.12 Fecha de vencimiento

La fecha de vencimiento de los dispositivos aprobados por PCI es la fecha en la que vence la aprobación del dispositivo. Todas las aprobaciones de dispositivos vencen de acuerdo con el siguiente calendario, excepto las de los SCRP. En el caso de estos últimos, las aprobaciones vencerán cinco años después de la fecha de aprobación.

Cuadro 6: Fechas de vencimiento de la aprobación

Versión de requisitos utilizada durante la evaluación en el laboratorio	Vencimiento de los requisitos	Vencimiento de la aprobación de los modelos de dispositivos
Versión 6.x de los*Requisitos de seguridad de PCI sobre PTS en los POI*	Por determinar en 2024	Abril de 2030
Versión 5.x de los *Requisitos de seguridad de PTS de POI de PCI*	Junio de 2021	Abril de 2026
Versión 3.x de los *Requisitos de seguridad de PCI sobre HSM*	Por determinar en 2021	Abril de 2026
Versión 4.x de los *Requisitos de seguridad de PCI sobre PTS en los POI*	Septiembre de 2017	Abril de 2023
Versión 2.x de los *Requisitos de seguridad de PCI sobre HSM*	Junio de 2017	Abril de 2022
Versión 3.x de los *Requisitos de seguridad de PCI sobre PTS en los POI*	Abril de 2014	Abril de 2021
Versión 1.x de los *Requisitos de seguridad de PCI sobre HSM*	Abril de 2013	Abril de 2019
Versión 2.x de los *Requisitos de seguridad de PCI sobre PED o EPP*	Abril de 2011	Abril de 2017
Versión 1.x de los *Requisitos de seguridad de PCI sobre UPT*	Abril de 2011	Abril de 2017
Versión 1.x de los *Requisitos de seguridad* de *PCI sobre PED o EPP*	Abril de 2008	Abril de 2014

Las aprobaciones para dispositivos evaluados por PCI vencen seis años después de la fecha de entrada en vigor de una actualización posterior de los requisitos de seguridad de PCI.

La fecha de vencimiento del la v6 del firmware del POI es a los tres años de su fecha de aprobación, siempre que no sea posterior al vencimiento de la aprobación general del dispositivo.

A.13 Características específicas por clase de aprobación

Cuadro 7: Características específicas

Característica y aplicación	Descripción
Soporte de PIN (PED, EPP, SCR, SCRP, UPT)	**"Soporte de PIN"** denota el tipo de verificación de entrada de PIN que admite el POI. "En línea" significa que el POI tiene la capacidad de admitir verificación del PIN en línea por medio del emisor de la tarjeta de pago o su procesador designado. Para superar las pruebas, los POI que admiten entrada de PIN en línea deben admitir el uso de TDES (estándar de cifrado de datos triple) o AES (estándar de cifrado avanzado) para proteger el PIN. Además, si el PIN debe protegerse durante su transporte en un POI sin conexión no integrado, entonces el POI debe admitir el uso de TDES y AES para ese canal. "Sin conexión" significa que el POI puede verificar PIN sin conexión por medio del chip integrado en la tarjeta de pago. A menos que se indique lo contrario, la designación "Sin conexión", sin otra especificación, en la *Lista de aprobación de dispositivos de PTS de PCI* significa que el POI puede admitir verificación de PIN sin conexión tanto en texto simple como cifrado. La designación "Sin conexión (p)" con la especificación "(p)" significa que el POI sin conexión puede realizar únicamente verificación de PIN sin conexión en texto simple. ***Nota:*** *Todos los POI de verificación de PIN sin conexión aprobados recientemente deben admitir verificación de PIN tanto en texto simple como cifrado.* No obstante, en virtud de las pruebas actuales, todos los POI sin conexión evaluados recientemente deben admitir verificación de PIN tanto en texto simple como cifrado. Los SCR u otros dispositivos de POI que incluyen un ICCR o un lector híbrido deben tener la designación "Sin conexión" para que se puedan utilizar para aceptación de PIN sin conexión.
Administración de claves de cifrado de PIN (PED, EPP, SCRP, UPT)	**"Administración de claves de cifrado de PIN"** indica si el laboratorio evaluó satisfactoriamente el dispositivo de seguridad de pago para admitir el uso de Triple DES (TDES) o AES para el cifrado de PIN para PIN en línea. TDES requiere el uso de al menos una clave de longitud doble. Una especificación de clave maestra (MK) o clave de sesión (SK), clave derivada única por transacción (DUKPT) y/o fija denotan que el dispositivo se ha evaluado satisfactoriamente para admitir la implementación de TDES para el esquema de administración de claves en cuestión. ***Nota:*** *DUKPT es el único algoritmo de clave única por transacción (UKPT) (ANSI X9.24) que PCI reconoce y aprueba; todas las demás formas de UKPT probadas por el laboratorio no se describirán en la carta de aprobación ni en el sitio web de PTS de PCI.*

Característica y aplicación	Descripción
	Si se utiliza el AES, se destacará explícitamente junto con las metodologías de MK/SK, DUKPT o clave fija. Esto aplica en dispositivos de POI que admiten la entrada de PIN en línea y, en general, esto no aplicará (N/A) en los dispositivos con la clase de aprobación Sin PED o SCR y, por definición, no aplicará para dispositivos de PIN solo sin conexión. ***Nota:*** *Los dispositivos de POI v5 y v6 utilizados para PIN en línea deben ser compatibles con el Formato 4 de Bloqueo de PIN establecido por la ISO (AES).*
Administración de claves SRED (PED, EPP, SCR, SCRP, UPT)	**"Administración de claves SRED"** indica si el laboratorio evaluó satisfactoriamente el dispositivo de seguridad de pago para admitir el uso de Triple DES (TDES) o AES para el cifrado de datos de cuentas. TDES requiere el uso de al menos una clave de longitud triple o DUKPT para el cifrado de datos de cuentas. Una especificación de clave maestra (MK) o clave de sesión (SK), clave derivada única por transacción (DUKPT) y/o fija denotan que el dispositivo se ha evaluado satisfactoriamente para admitir la implementación de TDES para el esquema de administración de claves en cuestión. Si se utiliza el AES, se destacará explícitamente junto con las metodologías de MK/SK, DUKPT o clave fija. Deberá especificarse FPE (cifrado de datos con preservación de formato) cuando se utilice uno de los algoritmos ANSI, ISO o NIST. ***Nota:*** *Esto aplica únicamente a dispositivos POI v6.*
Control de mensajes (PED, EPP, UPT)	▪ **Controlado por el proveedor:** El usuario final, el adquirente, o el revendedor no pueden modificar el firmware POI del punto de venta (POS) o la aplicación de pago del POI atendido para hacer cambios en los mensajes o los controles de entrada de PIN del dispositivo. Solo el fabricante de productos originales del POI tiene la facultad para modificarlos. ▪ **Controlado por el adquirente:** El fabricante de equipos originales envió el POI del POS atendido con mecanismos para controlar la pantalla del POI ya instalados. Estos mecanismos se pueden utilizar para desbloquear el POI para actualizar los mensajes del adquirente, usando procesos con controles criptográficos adecuados, como se define en el requisito de seguridad del POI pertinente. Si el revendedor o usuario final cuentan con la autorización del adquirente, también pueden hacer actualizaciones usando procesos con controles criptográficos adecuados. No aplica para dispositivos sin pantalla. Al implementarse, los dispositivos deben estar bloqueados. En todo caso, el cliente adquirente **siempre** tiene la responsabilidad de garantizar que existan procesos adecuados y procedimientos documentados para controlar la pantalla y uso del POI.

Característica y aplicación	Descripción
Tecnología con entrada de PIN (PED, EPP, UPT)	**"Tecnología con entrada de PIN"** indica la tecnología que está implementada para capturar el PIN de los titulares de tarjetas. El valor de este campo puede ser: ▪ **Teclado físico:** Conjunto de botones dispuestos en un bloque con dígitos y, opcionalmente, letras, de conformidad con la norma ISO 9564. ▪ **Pantalla táctil:** Pantalla que detecta la presencia y ubicación de un toque dentro de su área, y permite que los titulares de tarjetas ingresen su PIN. ▪ **N/A:** Para HSM, Sin PED, y para SCR y SCRP, excepto como se indique en estas dos últimas clases de aprobación. Un dispositivo no puede admitir tanto la versión del teclado físico como la de la pantalla táctil bajo la misma aprobación cuando ambos pueden usarse para entrada de PIN. Puede admitir un dispositivo que tiene ambas interfaces si se trata de respaldar leyes nacionales o locales deshabilitadas.
Componentes aprobados (PED, UPT)	**"Componentes aprobados"** contiene, si es pertinente, la lista de subcomponentes aprobados que forman parte del dispositivo aprobado, y que se han sometido satisfactoriamente a una evaluación inequívoca. Este componente se enumera con su número de aprobación. El uso de un dispositivo con componentes (p. ej., EPP, lectores de tarjetas) diferentes de los enumerados como componentes aprobados para el dispositivo en cuestión invalida la aprobación de dicho dispositivo.
Funciones proporcionadas (PED, EPP, UPT, SCR, SCRP, sin PED)	"**Funciones proporcionadas**" indica cuáles de las siguientes funciones admite el dispositivo. Pueden aplicar una o mas, dependiendo de la implementación: ▪ **Entrada de PIN:** El dispositivo permite la captura del PIN del titular de la tarjeta. ▪ **Capacidades del lector de tarjetas:** El dispositivo tiene componentes que pueden capturar datos de las tarjetas, tales como lectores de bandas magnéticas (MSR) o lectores de tarjetas con circuito integrado (ICCR) o sin contacto (CTLS). ***Nota:*** *Solo se considera que los lectores sin contacto cumplen con los requisitos para uso de cifrado de punto a punto (P2PE) si la clase de aprobación en cuestión se validó con el protocolo de SRED. Es más, algunas aprobaciones pueden ser de versiones validadas para SRED y algunas otras, no. Cuando sucede esto, solo los dispositivos que usan una versión de firmware designada para SRED se validan para satisfacer los requisitos de seguridad de los lectores sin contacto. En el caso de dispositivos con lectores sin contacto que usen firmware que no está validado para SRED, los requisitos de seguridad no serán validados.* ▪ **Pantalla:** El dispositivo tiene una pantalla integrada para mostrar mensajes dirigidos a los titulares de tarjeta y posiblemente alguna otra información. ▪ **SRED:** El dispositivo cumplió los requisitos de Lectura e intercambio seguros de datos. ▪ **OP:** El dispositivo cumplió con los requisitos aplicables de los protocolos abiertos.

Característica y aplicación	Descripción
Información adicional	En este campo se puede agregar otra información pertinente. Por ejemplo, cuando un proveedor cambió el estado de un dispositivo a “Descontinuado” (EOL), como se define en el inciso 5.4, “Tarifa de listado de aprobación” y, por ende, el dispositivo ya no está disponible para compra, excepto para fines de mantenimiento, sujeto a los reglamentos de la marca de pago. Los dispositivos cuyo estado es EOL ya no son respaldados por el proveedor y no se procesan deltas para dichos dispositivos. La fecha en que el estado de EOL entra en vigor se indicará en el sitio web. Esto también procederá para los HSM v2 y v3 para definir si se aprueban para uso restringido o no restringido, como se establece en los requisitos de seguridad para HSM. ▪ **Restricted:** La aprobación es válida solo cuando se implementa en entornos controlados o más robustos (p. ej., entornos seguros), como se define en la norma ISO 13491-2 y en la Política de seguridad de HSM de PCI del dispositivo. ▪ **No restringida:** La aprobación es válida en cualquier entorno. Los dispositivos que admiten bloqueo de PIN formato 4 de acuerdo con ISO (AES) se destacarán aquí. Para obtener más información sobre si se admiten las metodologías de MK/SK, DUKPT o clave fija para bloqueos de PIN del AES, consulte la sección Administración de claves.
Factor de forma del dispositivo	Todos los componentes relacionados con la seguridad (ensamblador de PIN, lectores de tarjeta) del dispositivo se muestran en una o más fotografías. Al menos, una de las fotografías debe cumplir con el requisito de que el número de versión del hardware debe mostrarse en una etiqueta adherida al dispositivo. Cabe destacar que para los dispositivos con varias versiones de hardware aprobadas, solo es necesaria una ilustración para que los compradores puedan determinar fácilmente la(s) versión(es) aprobadas.

Apéndice B: Evaluación de deltas – Guía de alcance

B.1 Introducción

El PCI SSC reconoce que es posible que los proveedores deban hacer correcciones de mantenimiento en los dispositivos validados por PTS que el proveedor ya vendió, pero a los cuales sigue brindando soporte. Además, es posible que los proveedores deseen transferir versiones actualizadas de firmware validado que se evaluaron con requisitos de seguridad más actuales a productos cuya aprobación ha vencido. Esto puede suceder cuando los clientes desean estandarizar sus implementaciones de acuerdo con una versión específica de firmware y/o agregar funciones a esos dispositivos.

Este apéndice brinda una guía sobre si los cambios realizados por los proveedores a un dispositivo de PTS validado (ya sea POI o HSM) tienen su alcance suficientemente delimitado, de manera que sea admisible que dichos cambios al dispositivo se puedan evaluar como una “delta” de la validación original. Todo cambio en el hardware de un dispositivo aprobado que se ha implementado debe derivar en un nuevo número de versión de hardware. Todo cambio en el firmware de un dispositivo aprobado debe derivar en una nueva versión de firmware. Los dispositivos deben someterse a una evaluación de deltas cuando se hagan tales cambios.

B.2 ¿Qué es una evaluación de deltas?

Todas las evaluaciones iniciales en virtud de una versión principal (p. ej., 1.x, 2.x, 3.x, 4.x, 5.x, 6.x, etc.) de los requisitos de seguridad de un producto dado deberán constituir una nueva evaluación y deberán recibir un nuevo número de aprobación.

Las modificaciones en los dispositivos aprobados se denominan “deltas”. En las revisiones de deltas participa el Laboratorio de PTS reconocido (o “Laboratorio de PTS”), el cual evalúa los cambios en función de la versión principal más actual de los requisitos de seguridad utilizada para la evaluación inicial y la publicación más reciente de preguntas frecuentes relacionadas con dichos requisitos. Por ejemplo, si un dispositivo inicialmente se evaluó con base en el PTS v6.0 del POI, cualquier evaluación de deltas tendría que realizarse usando la v6.1 (la versión más actual de PTS v6.x y las preguntas frecuentes v6.x emitidas más recientemente). Como ejemplos de deltas, podemos mencionar:

- Modificaciones en firmware o hardware actual en dispositivos aprobados anteriormente para agregar o modificar funciones.
- Adición de chip tipo EMV (Europay, MasterCard y Visa) nivel 1 en una aprobación actual.
- Correcciones de mantenimiento en dispositivos cuyas aprobaciones han vencido.
- Evaluación de un dispositivo con entrada de PIN sin conexión donde la aprobación actual solo incluye entrada de pin en línea o viceversa.
- Transferencia de un nuevo conjunto de firmware a un dispositivo actual aprobado.

La evaluación de deltas no puede considerar un producto aprobado previamente en virtud de una versión principal anterior del Estándar de PTS del POI —p. ej., 5.x— para una aprobación en virtud de otro número de versión principal —p. ej., 6.x—.

Las preguntas frecuentes solo deben abordar aspectos del dispositivo que resulta afectado por los cambios que hizo el proveedor. Por ejemplo, si un proveedor hiciera cambios en la disposición del hardware del diseño del POI, pero no modificara el firmware en absoluto, todas las entradas actualizadas en las preguntas frecuentes que afectan únicamente al firmware no se aplicarían en la evaluación de deltas. Esto se define más ampliamente en la sección “Proceso detallado de la evaluación” de la *Guía de pruebas y aprobación de los dispositivos PTS de PCI.*

B.3 Cómo determinar si es permisible una evaluación de deltas

No es posible prever la posibilidad de hacer cambios y conocer sus repercusiones de antemano. Los cambios deben evaluarse caso por caso. Se recomienda a los proveedores consultar a alguno de los Laboratorios de PTS para recibir orientación. Los Laboratorios de PTS consultarán a PCI según sea necesario antes de presentar un informe de deltas, a fin de determinar si un conjunto de cambios es demasiado amplio para abordarse en el proceso de deltas. Los laboratorios determinarán si el cambio afecta aspectos de seguridad. En todos los casos, este tipo de cambios requiere una evaluación que debe presentarse en el informe de deltas. Como mínimo, todos los requisitos que se identifican en el cuadro a continuación para cada tipo de cambio deben evaluarse en cuanto a su impacto en el aspecto de seguridad. En el informe de deltas, se debe presentar una justificación por cada cambio que se determine que no afecta el aspecto de seguridad.

B.3.1 Muestras de impactos de ciertos cambios

Las siguientes subsecciones pormenorizan una lista no exhaustiva de ejemplos de cambios que, si se consideran individualmente, se pueden considerar mediante el proceso de deltas. La inclusión de demasiados cambios, especialmente si se considera hacer una serie de modificaciones en el hardware del dispositivo, debe considerarse como un nuevo dispositivo que requiere una evaluación completa en virtud de la última versión del Estándar de PTS actual.

B.3.2 Cambios en el firmware

En general, todos y cada uno de los cambios realizados en el firmware que se ejecuta en un dispositivo de PTS aprobado anteriormente pueden considerarse en una sola evaluación de deltas, salvo si el cambio se considera demasiado generalizado, tal como un cambio en el sistema operativo —p. ej., cambiar de un sistema patentado a uno abierto—. El siguiente cuadro identifica diferentes tipos de cambios en el firmware y los requisitos de PTS que, como mínimo, deben considerarse al evaluar cada tipo de cambio. Los Laboratorios de PTS que evalúan tales cambios pueden justificar la exclusión de cualquier requisito identificado o la inclusión de otros requisitos con base en su evaluación.

Cuadro 8: Tipos de cambios en el firmware y requisitos afectados

Entre los cambios aceptables en el firmware que pueden considerarse en una evaluación de deltas, podemos mencionar:

Tipos de cambios en el firmware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**v6.x**
Cualquier cambio en el firmware	N/A	N/A	N/A	B20	B20	B20
Cambios en el firmware sin afectación evidente en los requisitos de PCI	B3	B3	B3, F1, G1, H1, I1	B3, F1	B3, F1	D2, E2
Modificaciones en la metodología segura de recuperación tras manipulación	B1	B1	B1	B1	B1	B1
Manejo de errores (es decir, desbordamiento de búfer)	A5, B2	A3, B2	A3, B2	A3, B2	A2, B2	A3, D1

Tipos de cambios en el firmware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**v6.x**
Modificaciones en los protocolos de comunicaciones externas	B2	B2	B2, F1, G1, H1, I1	B2, F1	B2, F1	D1, D2
Cambio en los mecanismos de actualización de software/firmware	B3, B4	B3, B4	B3, B4, J4	B3, B4, B4.1, J4	B3, B4, B4.1, J4	E2, B2, B2.1
Nuevo esquema de autenticación de firmware o aplicaciones	B4	B4	B4	B4, B4.1	B4, B4.1	B2, B2.1
Modificaciones en los tiempos de espera para ingresar PIN	B7, C3	B6, B10	B6, B10	B6, B10	B6, B10	B4, B8
Modificaciones en las funciones 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
Cambios no relacionados con la seguridad en el firmware de lectores de tarjetas	D4	A11, D4	A10, D4	A9, D4	A8, D4	A10, B21
Cambios en los mecanismos confidenciales de autenticación de servicios	B8, B9	B7, B8	B7, B8	B7, B8	B7, B8	B5, B6
Actualización de la metodología de carga de claves	C5	B11	B11, J4	B11, J4	B11, J4	B9, B2
Modificaciones en la administración de claves	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
Cambio en la jerarquía de claves	C1, C5, C7	B11, C1, D1	B11, C1, D1	B11, C1, D1	B11, C1, D1	B9, B18, A13
Modificaciones en el almacenamiento de claves	C1, C5	B11, D1	B11, D1	B11, D1	B11, D1	B9, A13
Nuevos tipos de claves	C1, C5, C6	B11, B13, D1	B11, B13, D1	B11, B13 D1	B11, B13 D1	B9, B12, A13
Modificaciones en el manejo de la longitud del PIN	C4, D4	B12, D4	B12, D4	B12, D4	B12, D4	B11, B21
Cambios menores en la interfaz de usuario	B5, B6	B5, B15	B5, B15, F1 G1, H1, I1	B5, B15, F1	B5, B15, F1	B3, B14, D2
Mensajes de PIN actualizados	A7, B5, B6	A8, B5, B15	B5, B15, B16	B5, B15, B16	B5, B15, B16	B3, B14, B15

Tipos de cambios en el firmware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**v6.x**
Incorporación de funcionalidad de SRED ***Nota:*** *No se aceptarán deltas de SRED en dispositivos v2.x después del 31 de diciembre 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 Cambios en el hardware

Los cambios realizados por los proveedores al hardware de dispositivos de PTS aprobados anteriormente son admisibles solo si el alcance de tales cambios es limitado. El siguiente cuadro identifica diferentes tipos de cambios en el hardware y los requisitos de PTS que, como mínimo, deben considerarse al evaluar cada tipo de cambio. Los Laboratorios de PTS que evalúan tales cambios pueden justificar la exclusión de cualquier requisito identificado o la inclusión de otros requisitos con base en su evaluación.

La inclusión de más de cuatro (4) de los tipos de cambios identificados y descritos en el cuadro a continuación en una sola presentación de deltas para un dispositivo de PTS aprobado anteriormente puede describir de manera eficaz a un nuevo dispositivo, que deberá someterse a su propia evaluación completa en virtud de la última versión del Estándar de PTS actual. Los cambios considerados para presentación de deltas que superen este umbral, que, en la opinión del Laboratorio de PTS, representen un cambio menor en el dispositivo de PTS aprobado, deben presentarse al PCI SSC antes de finalizar la evaluación a fin de determinar si su alcance es demasiado amplio. Asimismo, no es admisible proponer la presentación de una serie de deltas con cambios en el hardware con la intención de evitar dicho umbral. Si una presentación de deltas con cambios en el hardware se recibe dentro de un lapso de tres meses a partir de la aprobación del dispositivo de referencia, es necesario incluir suficiente información para justificar la necesidad de los cambios y la razón por la que no se incluyeron como parte de la presentación aprobada anteriormente. En todos los casos, los cambios acumulados se considerarán al evaluar la pertinencia de cualquier solicitud de una delta específica.

Por ejemplo, un proveedor hace un cambio en las rejillas contra manipulaciones y la ruta de las señales en seis placas de circuito impreso (PCB) de un dispositivo. De acuerdo con la guía de alcance de las deltas, la inclusión de cuatro o más tipos de cambios en el hardware en una sola presentación de deltas para un dispositivo de PTS aprobado anteriormente puede describir de manera eficaz a un nuevo dispositivo, que deberá someterse a su propia evaluación completa en virtud de la última versión del Estándar de PTS actual. En este ejemplo, esto no cuenta como seis cambios sino como uno solo, dado que todos pertenecen al mismo “tipo” de cambio. Esto cumple con los criterios de una delta.

Un dispositivo enviado con cambios internos de hardware suficientes para requerir una nueva evaluación —pero sin cambios externos— no puede presentarse como una delta, aunque su apariencia exterior sea idéntica. La magnitud de los cambios hechos internamente requiere que el dispositivo se someta a una evaluación completa en virtud de la versión de requisitos disponible actualmente para utilizar en evaluaciones nuevas. Si la evaluación es satisfactoria, derivará en un número de aprobación nuevo. Además, si bien el nuevo dispositivo tendrá una versión diferente de hardware de la del dispositivo actual, también deberá tener un nuevo nombre y número de modelo. Esto es para evitar confusiones en el mercado, especialmente si surgen problemas después de su implementación, que afecten solo a una de las aprobaciones pero no a las demás.

Reemplazar una PCB no se considera un solo cambio. Se deben considerar todos los cambios relacionados con el cambio en la PCB. Por ejemplo, hacer cambios en la PCB afecta a la rejilla contra manipulaciones y desvía las señales. Eso contaría como un cambio. Mover un procesador también contaría como un cambio y deberá evaluarse como corresponde. Cualquier otro cambio relevante en cuanto a la seguridad que derive de un cambio en la PCB también se incluiría en el conteo de cambios.

Todo cambio realizado en el hardware de un PED aprobado, incluso si no se hizo en componentes no relacionados con la seguridad, tiene el potencial de afectar directa o indirectamente la seguridad del dispositivo. Por definición, toda evaluación de deltas que incluya modificaciones en el hardware de un dispositivo aprobado —incluso en los circuitos no relacionados con las funciones de seguridad del dispositivo— debe, como mínimo, ser revisada por el Laboratorio de PTS en cuanto a su posible impacto en los siguientes requisitos de seguridad de la versión pertinente del Estándar de PTS en virtud del cual se está realizando la evaluación:

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

Tabla 9: Cambios aceptables en el hardware

Entre los cambios aceptables en el hardware que pueden considerarse en una evaluación de deltas, podemos mencionar:

Tipos de cambios en hardware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Cualquier cambio en el hardware[2]	A1, A2, A3, C1	A1, A7	A1, A7	A1, A6, B2, B20	A1, A5, B2, B20	A1, A2, A6, D1, B20

[2] Este elemento no debe incluirse en el conteo de cambios al determinar si la cantidad de cambios en una sola presentación de deltas se encuentra dentro del intervalo aceptable de cuatro (4) cambios. Todo cambio en el hardware requiere un cambio en el número de su versión, de acuerdo con el Apéndice A.

Tipos de cambios en hardware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Cambios en los plásticos de las carcasas (p. ej., dimensiones de la abertura de la cubierta, áreas que permiten acceso interno) o en las pantallas solo de salida. Los dispositivos modificados deben conservar el factor de forma original del dispositivo y la visibilidad de sus características.[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
Modificaciones en los interruptores contra manipulaciones o eliminaciones (p. ej., cambios en los materiales, rendimiento, ubicación, circuitos, repuesta a manipulaciones, etc.) o en las características de resistencia o a prueba de manipulaciones.	A5, D1	A2, A3, A11, D1	A2, A3, A10, D1	A2, A9 D1	A2, A8 D1	A3, A10, A13
Modificaciones o reemplazo de cualquier procesador utilizado por el 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
Cambios en las interfaces de usuario que podrían usarse para entrada de PIN (p. ej., pantallas táctiles, membranas, botones del teclado, etc., pero excluyendo las modificaciones en las teclas de función).	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

[3] "Características visibles" se refiere a la apariencia y sensación al tacto del dispositivo, incluidas sus dimensiones físicas. "Dimensiones físicas" se refiere al tamaño físico del dispositivo medido por su parte superior e inferior, o en el caso de un dispositivo circular, su circunferencia. Su ancho o grosor también se considera en las dimensiones físicas. Por ejemplo, la incorporación o eliminación de una impresora, pantalla LCD, lector de código de barras, o compartimento ampliado para baterías que cambia el grosor del dispositivo es aceptable, siempre y cuando no cambie el aspecto de la seguridad del mismo. Los cambios que se permitirán como delta no deben superar el 10% de la dimensión lineal más larga. Por ejemplo, un dispositivo que mide 10 pulgadas de largo puede cambiarse a no menos de 9 pulgadas o no más de 11 pulgadas como parte de una delta. No obstante, incluso como una delta, requerirá que se cambie el nombre del modelo, que se puede enumerar junto con la lista original.

[4] Cada modificación o reemplazo de un procesador cuenta como un cambio de hardware independiente (p. ej., si se modifican tanto el procesador seguro como el procesador de aplicaciones, se contarían como dos cambios en el hardware.).

Tipos de cambios en hardware	Requisitos afectados					
	Versión estándar de PTS					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Reemplazo o incorporación de cualquier lector [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
Modificaciones en los circuitos de comunicación	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
Modificaciones en los circuitos de energía	A5	A3	A3	A3	A2	A3
Modificaciones en otros componentes principales de los circuitos de la PCB (p. ej., circuitos de audio, circuitos del calentador de inducción, etc.). [6,7]	A5, A8	A3, A5	A3, A5	A3, A11	A2, A10	A3, B5

B.4 Contratación de un laboratorio PTS para la evaluación Delta

Los proveedores pueden elegir realizar una evaluación de deltas en un Laboratorio de PTS diferente al que recurrieron para realizar la evaluación inicial o antes de la evaluación de deltas. No obstante, el Laboratorio de PTS posterior ("Laboratorio de deltas") tiene la libertad de determinar el nivel de confianza del trabajo realizado por el Laboratorio de PTS anterior y asumirá la responsabilidad de cualesquier incumplimientos que arroje la revisión de deltas; esto puede derivar en más trabajo del necesario. En el caso de informes versión 3 o superior, el Laboratorio de deltas tendrá acceso a los informes del Laboratorio de PTS anterior, incluidos los informes de deltas o de componentes de OEM posteriores a la evaluación original. Si no recibe dichos informes, el Laboratorio de deltas rechazará la petición o deberá realizar una evaluación completa del dispositivo.

B.5 Requisitos de documentación Delta

B.5.1 Guía de presentación de informes para proveedores PTS

El proveedor de PTS debe divulgar todo cambio en los dispositivos de PTS aprobados. Se recomienda que los proveedores de PTS envíen un documento de Análisis de cambios al Laboratorio de PTS que contenga, mínimo, la siguiente información:

- Nombre del dispositivo de PTS;

[5] Cada cambio de lector cuenta como un cambio de hardware independiente —p. ej., si se cambian tanto el MSR como el ICCR, cuenta como dos cambios en hardware—. Sin embargo, el cambio en un lector híbrido cuenta como solo un cambio en hardware.

[6] Esto excluye el enrutamiento de los circuitos.

[7] El reemplazo o rediseño total de una PCB que agrega o elimina funciones o características de seguridad requiere una evaluación completa.

- Números de versión de hardware, firmware y aplicación, según corresponda, para ser evaluados;
- Datos del dispositivo de PTS aprobado actualmente en la Lista de dispositivos PTS aprobados, usado como referencia para la evaluación;
- Datos del Laboratorio de PTS que realizó la evaluación original del dispositivo, e información sobre evaluaciones de deltas posteriores realizadas en el dispositivo desde su aprobación inicial;
- Descripción del cambio;
- Razón por la que es necesario el cambio;
- Explicación de cómo funciona el cambio;
- Explicación sobre cómo y por qué resultan afectados los requisitos de PTS;
- Descripción de las pruebas que realizó el proveedor para validar cómo se ven afectados los requisitos de seguridad de PTS; y
- Descripción de cómo la identificación (control de versiones) del cambio encaja en la metodología de control de la configuración del proveedor.

B.5.2 Requisitos para la presentación de informes para laboratorios PTS

Los informes de evaluación de deltas deben presentar toda la información pertinente sobre los cambios y la evaluación de los mismos, equivalente a los niveles de detalles especificados en los requisitos de prueba derivados (DTR). Los Laboratorios de PTS deben proporcionar la siguiente documentación con cada delta que presentan:

- La cantidad de tipos de cambio en hardware identificados.
- Una descripción amplia que defina claramente todos los cambios que se realizaron en el dispositivo de PTS aprobado.
- Citas de:
  - El informe de aprobación de referencia y cualesquier presentaciones de deltas posteriores en las que se basa la presentación de la delta actual.
  - Documentación complementaria para fundamentar las conclusiones que se incluyen en la presentación de deltas.
- Un cuadro que proporcione la siguiente información acerca de cada cambio expresado en la actualización del dispositivo de PTS aprobado a partir de la configuración aprobada anteriormente:
  - Descripción del cambio;
  - Identificación del elemento o elementos de la configuración enmendado(s) (archivos del sistema o componentes de hardware) que resultan afectados por el cambio;
  - Una evaluación amplia de cómo afecta el cambio el aspecto de seguridad;
  - Identificación de los requisitos de seguridad de PTS que resultan afectados por el cambio (incluidos los requisitos para los cuales las respuestas anteriores permanecen sin cambio); y
  - Una descripción amplia de las pruebas realizadas, de haberlas, para validar la evaluación;
- Las respuestas actualizadas de los requisitos de seguridad de PTS afectados que claramente describen cambios que son necesarios para las evaluaciones de referencia.

B.6 Aplicabilidad de las Preguntas frecuentes durante las evaluaciones Delta

Las preguntas frecuentes (FAQ) técnicas se actualizan periódicamente, no solo para puntualizar los requisitos a fin de proporcionar un terreno congruente y con igualdad de condiciones en las aplicaciones de esos requisitos, sino también para abordar nuevas amenazas de seguridad que vayan surgiendo. Por tal motivo, las Preguntas frecuentes técnicas generalmente entran en vigor inmediatamente al momento de su publicación.

La intención no es evitar que un dispositivo que está en evaluación apruebe debido a la publicación de las Preguntas frecuentes posteriores a su aprobación. Sin embargo, esto puede ser necesario si existen vulnerabilidades de seguridad que cambian considerablemente las amenazas para el dispositivo a partir de cuando se evaluó originalmente. A menos que existan una o más de tales vulnerabilidades, un producto que actualmente está en evaluación, por lo general, no se someterá a nuevas Preguntas frecuentes emitidas durante la evaluación del producto. Esto no exime a un producto de la pertinencia de las Preguntas frecuentes si el producto debe revisarse y volverse a presentar en una fecha posterior debido a otros problemas que causaron que no aprobara la evaluación.

Los dispositivos que se sometan a evaluaciones de delta deben tomar en cuenta las Preguntas frecuentes actuales de la versión principal de los requisitos de seguridad solo de los requisitos de seguridad que resultan afectados por la delta. Por ejemplo, si un cambio afecta el cumplimiento con los requisitos B1 y B4, solo deben tomarse en cuenta las Preguntas frecuentes asociadas con B1 y B4 como parte de la delta.

Además, no basta con que el laboratorio determine que el cambio no reduce la seguridad del dispositivo. Debido a la evolución de las amenazas y las técnicas de ataque a partir del momento en que se hizo la evaluación original (que puede haber sucedido muchos años antes), el laboratorio debe determinar si el dispositivo sigue cumpliendo con los requisitos de seguridad pertinentes que resultaron afectados por el cambio, dados los cambios en los vectores de ataque. Esto es porque, ya sea que las deltas se hagan para mejorar o corregir la funcionalidad o para otros fines, la intención es extender la vida del dispositivo en el mercado.

En todos los casos, el Laboratorio de PTS que realiza la evaluación debe notificar las circunstancias al PCI SSC, y este tomará la decisión final con base en ellas. Además, tanto para las evaluaciones nuevas como de deltas, el Laboratorio de PTS también indicará en su presentación la versión de los requisitos de seguridad utilizada en las evaluaciones, así como la fecha de publicación de las Preguntas frecuentes técnicas que se aplicaron.

B.7 Consideraciones sobre los componentes actualizados en terminales integradas

Los proveedores con dispositivos de PTS aprobados que integran otros componentes OEM aprobados por PTS (tales como las UPT) pueden buscar evaluaciones de deltas para tales dispositivos en el caso de cambios que se hacen en los componentes OEM integrados, incluyendo el reemplazo de cualquier componente OEM dado con un modelo diferente (p. ej. un ICCR OEM aprobado por separado producido por un proveedor se sustituye en el factor de forma final de la terminal integrada o UPT con un modelo diferente, aún si es de otro proveedor). Esta concesión aplica siempre y cuando el proveedor conserve el control del ensamblaje final y la fabricación de la terminal integrada o UPT.

Los cambios que se generen en el propio factor de forma final (p. ej., la carcasa) debido a la complejidad de la integración deben someterse a pruebas, como una nueva evaluación en virtud de una versión de los requisitos cuyo uso no se haya retirado para nuevas evaluaciones.

No obstante, en todos los casos se evaluarán los requisitos de seguridad que se vieron afectados, incluyendo los que no se aplicaban anteriormente (p. ej., si la nueva carcasa presenta dispositivos adicionales de interfaz del titular de la tarjeta que no estaban presentes en la evaluación original).

Apéndice C: Solicitud de cambio administrativo en PTS

Los cambios administrativos que afectan a un dispositivo de PTS aprobado, el nombre o dirección comercial de proveedores de PTS o información de contacto deben divulgarse en este documento de *Cambio administrativo*. Los proveedores deben llenar cada sección y luego enviar el documento a un Laboratorio reconocido de PCI. El laboratorio, a su vez, debe enviar la documentación complementaria requerida mediante un Cambio administrativo al PCI SSC para su revisión. Para los cambios que incluyen imágenes nuevas, estas deben enviarse mediante una presentación de delta.

Información sobre el proveedor de PTS			
Nombre de la empresa		Fecha de presentación	
Nombre del solicitante del cambio		Correo electrónico:	
Puesto del solicitante del cambio		Función (Primaria, facturación, técnica)	

Descripción de los cambios				
Tipo de modificación (marque todas las opciones que correspondan)	☐ Nombre de la empresa	☐ Dirección de la empresa	☐ Nombre(s) del modelo del dispositivo	☐ Nombre/Dirección de contacto
Describa brevemente el motivo de la modificación				

Información corregida de la empresa			
Nuevo nombre de la empresa		Nuevo sitio web	
Dirección postal			
Dirección de facturación			

Modelo(s) del dispositivo			
Número de aprobación de PTS	**Nombre del modelo**	**Información sobre el nuevo modelo**	
		Nombre del modelo nuevo	Imagen incluida *
			☐
			☐
			☐
			☐
			☐
			☐

Modelo(s) del dispositivo			
Número de aprobación de PTS	**Nombre del modelo**	**Información sobre el nuevo modelo**	
		Nombre del modelo nuevo	Imagen incluida *
			☐
			☐
			☐
			☐

** En "Imágenes del nuevo modelo de dispositivo" en la última página.*

Contacto principal o comercial			
Nombre del contacto		Puesto	
Correo electrónico de contacto		Teléfono de contacto	

Contacto de facturación *(las facturas se enviarán a esta persona o correo electrónico)*			
Nombre del contacto		Puesto	
Correo electrónico de contacto		Teléfono de contacto	

Contacto técnico			
Nombre del contacto		Puesto	
Correo electrónico de contacto		Teléfono de contacto	

Documentación de soporte requerida

	Cambio administrativo (este formulario)	Política de seguridad	Convenio de descargo del proveedor (VRA)	Imágenes del dispositivo*
Cambio del nombre de la empresa	**X**	**X**	**X**	**X**
Nombre del modelo del dispositivo	**X**	**X**		**X**
Nombre del contacto principal	**X**			

** Si corresponde, las imágenes deben enviarse mediante una presentación de delta.*

Apéndice D: Certificación de validación PTS

Instrucciones de presentación

El proveedor de PTS debe llenar este documento como una declaración del estado de validación del firmware con los requisitos de seguridad de PTS de POI o de HSM, según corresponda. No se requiere que los proveedores y otros terceros que concedan licencias de los productos aprobados de otros proveedores para comercializarlos o distribuirlos con sus propios nombres llenen esta certificación cuando las licencias no hagan cambios en el firmware, salvo al hacer actualizaciones con base en las modificaciones que el proveedor OEM haya hecho a su propio producto, en el cual se basa el producto autorizado.

El proveedor de PTS deberá llenar todas las secciones pertinentes y enviar este documento junto con copias de todos los documentos de validación requeridos a PCIPTS@pcisecuritystandards.org, de acuerdo con las instrucciones del PCI SSC para la presentación de informes, como se describe en la *Guía del programa de pruebas y aprobación de dispositivos de PTS*.

Parte 1. Proveedor de PTS					
Nombre de la empresa:					
Nombre del contacto:			Puesto:		
Teléfono:			Correo electrónico:		
Dirección de la empresa:			Ciudad:		
Estado/Provincia:		País:		Código postal:	
URL:					

Parte 2. Información sobre la aprobación de dispositivos

Para cada aprobación de HSM o POI que no haya vencido a partir del año anterior, terminando el 31 de diciembre, indique el estado de presentación de firmware como:

A: No se han hecho modificaciones a la versión del firmware.

B: Todos los cambios en hardware y firmware fueron evaluados por un Laboratorio de PTS en un informe enviado a PCI, incluidas las versiones de hardware o firmware donde se indica que usan una metodología de control de versiones comodín aprobada. Esto incluye, para todos los dispositivos POI, todas las vulnerabilidades identificadas por el proveedor en cada uno de los protocolos e interfaces definidos en el requisito de seguridad D1 del POI, como demuestra el proceso de evaluación de vulnerabilidades definido en los requisitos E10 a E12 de los DTR de POI.

Para los dispositivos compatibles con protocolos abiertos, el proveedor deberá entregar materiales probatorios de que existe un registro auditable del proceso de evaluación de vulnerabilidades en curso proporcionando una copia del formulario de aprobación del proveedor especificado en el Requisito E10 de POI para el año anterior, que termina el 31 de diciembre.

Número de aprobación de PTS	Fecha de vencimiento de la aprobación	Nombre del modelo	Verificación de firmware	Estado de presentación del firmware durante los 12 meses, terminando el 31 de diciembre del año anterior	
				A	B
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐

Parte 3. Confirmación del proveedor de PTS	
Firma del funcionario ejecutivo del proveedor de PTS ↑	*Fecha ↑*
Nombre del funcionario ejecutivo del proveedor de PTS ↑	*Cargo ↑*
Empresa representada por el proveedor de PTS ↑	

Apéndice E: Certificación del dispositivo PTS

El proveedor de PTS debe llenar este documento como una declaración del estado de validación del dispositivo con los requisitos de seguridad de PTS de POI. El proveedor de PTS deberá llenar todas las secciones pertinentes y enviar este documento a solicitud del comprador.

Parte 1. Proveedor de PTS					
Nombre de la empresa:					
Nombre del contacto:			Puesto:		
Teléfono:			Correo electrónico:		
Dirección de la empresa:			Ciudad:		
Estado/Provincia:		País:		Código postal:	
URL:					

Parte 2. Información sobre la aprobación de dispositivos

Indique en cada dispositivo pertinente el estado de presentación del hardware y firmware como:

A: No se han hecho modificaciones a las versiones de hardware o firmware, como se enumeran en el sitio web de PCI.

B: Todos los cambios en hardware y firmware fueron evaluados por un Laboratorio de PTS en un informe enviado a PCI, incluidas las versiones de hardware o firmware donde se indica que usan una metodología de control de versiones comodín aprobada.

Número de aprobación de PTS	Nombre del modelo	Tipo A o B	Versión de hardware	Verificación de firmware	Versión de la aplicación (si corresponde)
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			

Parte 3. Confirmación del proveedor de PTS

Firma del funcionario ejecutivo del proveedor de PTS ↗	*Fecha ↗*
Nombre del funcionario ejecutivo del proveedor de PTS ↗	*Cargo ↗*

Empresa representada por el proveedor de PTS ↗