Industria de tarjetas de pago (PCI)

Requisitos de seguridad de PTS POI

Preguntas frecuentes técnicas para su uso con la versión 6

Septiembre de 2020

Índice

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.

Evaluación del dispositivo POI: preguntas frecuentes

Este documento de preguntas técnicas frecuentes contiene respuestas a las preguntas sobre la aplicación de los requisitos de seguridad de los dispositivos POI físicos y lógicos de la industria de tarjetas de pago (PCI), tal como se abordan en el manual *Requisitos de seguridad del dispositivo de punto de interacción PTS de PCI* . Estas preguntas frecuentes incluyen aclaraciones adicionales y oportunas para la aplicación de los requisitos de seguridad. Las preguntas frecuentes son parte integral de esos requisitos y se tendrán en cuenta plenamente durante el proceso de evaluación.

Actualizaciones: para mayor claridad, las preguntas nuevas o modificadas están en color **rojo.**

Preguntas generales

P 1 **Si una aplicación de un dispositivo incluye avisos de datos sin PIN y el dispositivo aplica los controles de conformidad con el requisito B15 de PCI, ¿puede aparecer como un dispositivo de avisos controlado por el adquirente con la aplicación excluida de los identificadores del dispositivo?**

A *Sí, en caso de que una aplicación no pueda cubrir las funcionalidades necesarias para cumplir con los requisitos de PCI. No es necesario que el código dentro del dispositivo que no proporciona ni puede afectar la seguridad esté representado por los identificadores del dispositivo aprobado.*

P 2 **¿Se asume que la superficie de la zona encapsulada es visible sin desmontar el dispositivo?**

A *No. Los componentes encapsulados y sensibles a la seguridad del dispositivo están dentro de la carcasa y, por lo tanto, es poco probable que sean visibles si esta no se abre.*

P 3 **¿Es aceptable que un dispositivo incluya componentes extraíbles y complementos proporcionados por el proveedor?**

A *Todos los componentes extraíbles (escudos de privacidad, estaciones de acoplamiento, módulos de interfaz, etc.) deben evaluarse en un laboratorio aprobado para determinar que no representan riesgos adicionales para la seguridad. Sin embargo, los componentes individuales no recibirán una aprobación independiente.*

P 4 **Febrero de 2014 (actualización): ¿el uso de superposición protectora sobre el teclado afecta el estado de aprobación de un dispositivo?**

A *Sí. En general, las superposiciones no cumplen con el programa de aprobación de dispositivos, ya que existe la posibilidad de que se haga una interceptación del teclado o se oculten evidencias de manipulación. Pueden utilizarse superposiciones si no cubren ninguna parte del área de entrada de PIN. Por ejemplo, en un dispositivo con pantalla táctil en el que esta se utiliza tanto para la captura de la firma como para la entrada de PIN, puede utilizarse una superposición para proteger el área de la firma del desgaste excesivo. En este ejemplo, solo puede protegerse la zona que se utiliza para la captura de la firma. El material utilizado debe ser transparente y no solo translúcido, de modo que no obstruya el área de entrada de clave cuando se visualice desde cualquier ángulo.*

P 5 **Diciembre de 2017 (actualización): ¿el uso de una funda protectora afecta el estado de aprobación de un dispositivo?**

A *Sí. En general, las fundas no cumplen con el programa de aprobación de dispositivos, ya que existe la posibilidad de que se oculten las evidencias de manipulación. Pueden utilizarse fundas cuando no cubren ninguna parte del área de MSR o ICCR. Por ejemplo, es posible que una funda que se utiliza para proteger un dispositivo móvil de caídas o la incorporación de un cordón no cubran el ICCR o el MSR. Las interfaces deben ser claras y visibles para el consumidor, de manera que no puedan ocultarse los cables o las evidencias de manipulación. El material utilizado debe ser transparente, no solo translúcido. Las superposiciones para el área de entrada de PIN deben cumplir con la anterior pregunta frecuente. Si se aprobó el POI para su uso con una funda protectora, la política de seguridad establecerá una imagen de una funda protectora aprobado, tal y como se haya instalado y probado correctamente en el laboratorio.*

P 6 **Mayo (actualización) 2018: ¿la entrada del código de autenticación (por ejemplo, la contraseña) que se utiliza para la liquidación/compensación en un cajero automático requiere el uso del EPP seguro o puede utilizar un mecanismo alternativo, como el teclado, en la parte posterior del cajero automático?**

A *La entrada del código de autenticación utilizado para la liquidación o compensación en el cajero automático no necesita capturarse a través del EPP, y puede utilizar el teclado instalado en la parte posterior del cajero automático. Sin embargo, en ningún caso se permiten las claves utilizadas para el cifrado de los PIN de titulares de tarjetas en relación con una transacción financiera para cifrar este código de autenticación. Las claves de cifrado PIN que se utilizan para la protección de los PIN de titulares de tarjetas no deben utilizarse para proteger el código de autenticación de liquidación, ya sea que ese valor se introduzca desde la parte posterior o a través del EPP. Para la protección del código de autenticación de la liquidación, habría que utilizar una clave de datos independiente.*

Tenga en cuenta que los códigos de autenticación ingresados para colocar el EPP en un estado confidencial, como los que se utilizan para permitir la carga manual de la clave, deben capturarse a través de una interfaz segura, es decir, a través del EPP.

P 7 **Algunos dispositivos se envían con firmware que puede transformarse en una versión compatible, pero que no cumple con los requisitos de envío. ¿Cuándo es aceptable esto?**

A *Esto solo es aceptable cuando la conversión es unidireccional y no puede revertirse. Un dispositivo solo puede convertirse a una versión compatible. No podrá convertir una versión compatible a una versión no compatible. La conversión debe realizarse al cargar la clave inicial de las claves secretas de la entidad adquirente. La transformación debe tener como resultado la puesta a ceros de cualquier clave secreta de entidad adquirente previa. La versión compatible del firmware debe distinguirse con claridad de la versión no compatible. No es aceptable simplemente añadir un sufijo (uno o más caracteres) a una versión de firmware actual. En vez de esto, la conversión debe tener como resultado un número de versión de orden superior que sea claramente distinguible para los compradores de dichos dispositivos. Solo se aprobará y enumerará la versión que cumpla con los requisitos.*

P 8 **Algunos ataques son técnicamente simples, ya que no requieren una identificación extensa, como interceptar una comunicación en interfaces estándar como USB/Ethernet entre dispositivos. En ese caso, ¿cómo se realizará el cálculo del valor de ataque?**

A *Para ataques técnicamente simples que no requieren una identificación extensa, como interceptar una comunicación en interfaces estándar como USB/Ethernet entre dispositivos, deben ignorarse todos los factores de costo, además del tiempo y la experiencia. Asimismo, el tiempo de ataque y la experiencia deben considerarse solo para identificar la configuración general del dispositivo y la propiedad que se va a atacar (por ejemplo, el tipo de interfaz).*

P 9 **La versión 1 de la UPT ya no estaba disponible para nuevas evaluaciones después de abril de 2011. ¿En qué condiciones se permite una UPT aprobada en la versión 1?**

A *Un proveedor con una aprobación general de la UPT versión 1 puede obtener deltas en ese dispositivo por los cambios que se produzcan en los componentes OEM utilizados, incluyendo la sustitución de cualquier componente OEM por un modelo diferente; por ejemplo, un ICCR OEM aprobado por separado que produzca un proveedor se sustituye en la UPT de factor de forma final por un modelo diferente, aunque sea de otro proveedor. Esto se aplica siempre que el proveedor siga teniendo control sobre el ensamblaje final y la fabricación de la UPT.*

Los cambios que se generen en el propio factor de forma final (por ejemplo, la carcasa) debido a la complejidad de la integración deben someterse a pruebas, como una nueva evaluación frente a una versión de los requisitos que no se haya retirado del uso para las 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; por ejemplo, si la nueva carcasa presenta dispositivos adicionales de interfaz del titular de la tarjeta que no estaban presentes en la evaluación original.

P 10 **¿Hay alguna diferencia si el proveedor de componentes OEM es también el proveedor que obtiene la aprobación general de UPT frente a un escenario en el que el proveedor OEM vende sus componentes/módulo de entrada a otros proveedores, como los proveedores de quioscos o de la AFD, que luego buscan una aprobación general de UPT?**

A *No. Los componentes OEM pueden fabricarse con cualquier proveedor, incluso si es diferente al de UPT. Sin embargo, si fuera el caso, esos componentes deben estar aprobados por PCI o bien, el proveedor del OEM debe otorgar permiso al proveedor de UPT para que esos componentes sean evaluados como parte de la aprobación general de UPT.*

P 11 **Junio de 2012: durante una evaluación, se determina que un nuevo dispositivo incluye la pila de IP idéntica, previamente evaluada y aprobada según la versión más reciente del módulo Requisitos de protocolos abiertos. ¿Es necesario volver a realizar todas las pruebas de los Protocolos abiertos?**

A *Si el vendedor es capaz de proporcionar evidencias que apoyen la afirmación de que la pila de IP es 100 % idéntica, incluyendo la misma versión de varios componentes y protocolos de IP, servicios de IP y protocolos de seguridad de IP idénticos, no es necesario realizar nuevas pruebas. El informe debe documentar cómo se verificó que la pila de IP es idéntica e incluirá la información de esta, como la versión del componente, los protocolos de IP, los servicios de IP y los protocolos de seguridad de IP compatibles.*

P 12 **Julio de 2014: los dispositivos POI pueden aprobarse con compatibilidad con Protocolos abiertos. Los proveedores proporcionan una política de seguridad establecida por PCI y otra guía de seguridad para la aplicación adecuada de los Protocolos abiertos que forman parte de la aprobación. Si la entidad que implementa el dispositivo hace cambios que no están de acuerdo con la guía de seguridad necesaria para implementar el dispositivo en conformidad con el módulo de protocolos abiertos, ¿esto afecta la aprobación? Por ejemplo: incluir servicios o protocolos adicionales que no se enumeraron en la guía o utilizar o reemplazar la pila de IP por una integrada en la aplicación.**

A *Sí, esto invalidaría el estado de aprobación del dispositivo para cualquier implementación que realice dichos cambios. Todo cambio de este tipo debe tener como resultado que el dispositivo se someta de manera satisfactoria a una evaluación delta para mantener la aprobación.*

El módulo de Protocolos abiertos es para garantizar que los protocolos y servicios abiertos en los dispositivos POI no tengan vulnerabilidades que puedan aprovecharse de forma remota, y que generen acceso a datos o recursos confidenciales en el dispositivo. En ese sentido, no importa con qué tipo de red (pública o privada) se utilice el dispositivo.

El proveedor define qué protocolos y servicios son compatibles con el dispositivo y establece una guía para su uso. El laboratorio evalúa los protocolos y servicios. La incorporación o habilitación de servicios y protocolos adicionales o el incumplimiento de la guía de seguridad emitida después de la evaluación invalidaría el estado de aprobación de ese dispositivo para esa aplicación.

P 13 **Enero de 2015: hay varias preguntas frecuentes sobre el uso de tecnologías inalámbricas, como Bluetooth y wifi. ¿Cuál es el objetivo de estas preguntas frecuentes? ¿PCI tiene algún requisito específico para otros tipos de tecnologías de la comunicación?**

A *La intención de las preguntas frecuentes sobre todas las comunicaciones inalámbricas para los dispositivos POI es garantizar que las interfaces de los POI estén protegidas de tal manera que:*

- *Los datos de la tarjeta no puedan interceptarse fácilmente.*
- *No pueda accederse fácilmente a las interfaces de comando de la terminal, interceptadas para ataques (como MITM) o que se utilizan como un vector de ataque en el dispositivo.*
- *El riesgo de la interfaz no causa, ni respalda ni facilita el riesgo adicional de los activos de seguridad del POI.*

PCI no exige ni requiere el uso de una tecnología de comunicación específica, pero cualquier implementación debe cumplir con los requisitos anteriores mediante algún aspecto de las capas físicas o lógicas de comunicación. La comunicación directa por cable o física a menudo logra esto a través de la naturaleza de su interfaz física. Las comunicaciones inalámbricas no pueden depender de esto sino, más bien, de la seguridad en el enlace o las capas de aplicación mediante el uso de un Protocolo de seguridad para establecer una ruta confiable para todas las comunicaciones a través del enlace inalámbrico. Este Protocolo de seguridad debe haberse probado y aprobado según el módulo de protocolos abiertos de la evaluación PCI PTS de ese dispositivo. Algunos ejemplos de implementaciones aceptables del protocolo de seguridad son WPA2 (en la capa del enlace) o túneles cifrados de VPN (en la capa de la aplicación).

P 14 Diciembre (actualización) de 2016: ¿puede usarse un dispositivo PTS como transmisor de baliza (iBeacon o baliza BLE)?

A *Están permitidas las balizas para cualquier versión de BLE (por ejemplo, 4.0, 4.1) siempre y cuando existan las siguientes condiciones y las valide un laboratorio aprobado por PTS:*

- *La baliza está aprobada como una interfaz de dispositivo en el informe PTS POI.*
- *El aprovisionamiento por aire (OTA, por sus siglas en inglés) no está permitido en ningún momento. El aprovisionamiento y la actualización de balizas deben cumplir con las normas de PTS (es decir, la Sección J, B4 o B4.1)*
- *Debe mencionarse en la política de seguridad.*
- *Las balizas son solo de transmisión. El laboratorio debe validar que la comunicación BLE no puede utilizarse para responder a cualquier solicitud externa, conectarse, emparejar o proporcionar de otro modo comunicación bidireccional a cualquier otro dispositivo.*
- *El proveedor proporciona la documentación sobre el uso seguro y el aprovisionamiento de la baliza, y dicha documentación establece claramente que la baliza se utiliza solo para transmisión y que no se permite el aprovisionamiento de OTA.*
- *El proveedor documentará el propósito de usar la funcionalidad de baliza, es decir, su uso previsto. La documentación debe incluir los datos que se transmiten y garantizar que no puedan transmitirse datos confidenciales.*
- *El dispositivo PTS nunca puede recibir transmisiones de baliza.*

P 15 ¿Con qué requisitos debe validarse un lector de tarjetas seguro?

A *Los SCR deben cumplir, según corresponda, los requisitos de ICCR y/o MSR designados en el Apéndice B de los requisitos de seguridad de PCI PTS POI y todos los demás requisitos relativos a la protección de los datos de la cuenta, conforme se establecen en el Apéndice B. Además, debe considerarse la aplicabilidad de todos los requisitos de protección de datos de cuenta no designados. En la mayoría de los casos no serán aplicables y no requerirán ninguna evaluación adicional a esa determinación.*

Si el dispositivo es capaz de comunicarse a través de una red IP o utiliza un protocolo de dominio público (como, por ejemplo, wifi o bluetooth), también deben cumplirse los requisitos especificados en el módulo de Protocolos abiertos. Pueden aplicarse otros requisitos, como B1, pruebas automáticas y B7, y números aleatorios dependiendo de la funcionalidad del dispositivo. En todos los casos en que se ve afectado un requisito de seguridad, es necesario evaluar el dispositivo con respecto a ese requisito.

P 16 Febrero de 2014: ¿puede usarse un SCR para la aceptación de PIN sin conexión?

A *Los SCR u otros dispositivos POI que incluyan un lector ICCR o un lector híbrido deben tener designado "sin conexión" en el soporte de PIN para poder utilizarse para la aceptación de PIN sin conexión.*

P 17 Febrero de 2014: si un SCR procesa PIN, es decir, admite la autenticación de PIN sin conexión a través de un componente del ICCR, o formatea y cifra un bloque de PIN para enviarlo en línea directamente al host, ¿debe evaluarse con un dispositivo específico de entrada de PIN?

A *Sí, debe validarse junto con un dispositivo específico de entrada de PIN,—por ejemplo, PED o EPP—para validar la seguridad de la interacción, incluyendo el establecimiento de la relación de claves. El dispositivo de entrada de PIN debe aprobarse previamente u obtenerse la aprobación al mismo tiempo que el SCR en la misma evaluación de laboratorio o en una evaluación simultánea por separado.*

P 18 Junio de 2012: los requisitos de aprobación de un dispositivo SCR o sin PIN no incluyen el PCI PTS DTR A1, que establece los mecanismos activos de respuesta a la manipulación. Si se puede demostrar que el costo del ataque supera los niveles mínimos requeridos para cada uno de los requisitos de pruebas de seguridad física, ¿es posible cumplir con los requisitos de seguridad física de un dispositivo SCR o sin PIN utilizando únicamente características de resistencia a manipulación y pruebas de manipulación?

A *No, es un requisito que todos los dispositivos implementen mecanismos de detección de manipulaciones activas para cumplir con los requisitos de seguridad física de PCI PTS. Los dispositivos SCR y sin PIN deben tener mecanismos de detección de manipulaciones permanentemente activos que vigilen la intrusión, y respondan ante tales eventos borrando de inmediato la información confidencial dentro del dispositivo, lo cual inhabilita el dispositivo.*

Un dispositivo no puede cumplir con los requisitos de PTS POI si no tiene un mecanismo activo de respuesta a la manipulación para poner a ceros las claves secretas y privadas durante un ataque de penetración, independientemente de qué módulo de la norma PTS POI esté diseñado para que el dispositivo pueda cumplirlo. La penetración del dispositivo debe borrar de manera automática e inmediata cualquier clave secreta y privada, de manera que no sea posible recuperar el material de la clave. Esto es aplicable para los dispositivos, incluso si no aceptan los PIN de los clientes, o no están diseñados para la protección de los PIN de los clientes. Las claves criptográficas secretas o privadas que nunca se utilizan para cifrar o descifrar datos, o que no se utilizan para la autenticación, están excluidas de este requisito, ya que nunca estarían involucradas en la protección de los PIN o los datos de las tarjetas de los clientes.

P 19 Julio de 2013: ¿puede aprobarse un dispositivo con un ICCR para el PIN en línea solo si admite cualquier método de introducción de PIN sin conexión (es decir, el dispositivo admite PIN cifrado y/o de texto plano)?

A *Los dispositivos con ICCR que no se evalúan conforme a los requisitos del ICCR para estar sin conexión no pueden tener la versión aprobada del firmware que cumple con la aceptación de cualquier PIN sin conexión. Además, los dispositivos que admiten el PIN en línea deben evaluarse en línea o bien, la versión aprobada del firmware debe tener desactivada la aceptación del PIN en línea.*

P 20 **Junio de 2012: si un dispositivo admite varias interfaces habilitadas por IP, ¿deben realizarse pruebas en todas las interfaces habilitadas por IP en el laboratorio durante la evaluación?**

A *Si un dispositivo es compatible con varias interfaces habilitadas por IP y la pila de IP (incluyendo todos los protocolos de IP, servicios de IP y protocolos de seguridad de IP) son idénticos para todas las interfaces, solo es necesario realizar pruebas en una de las interfaces habilitadas por IP.*

P 21 **Diciembre de 2013: los requisitos de PCI PTS no determinan ningún factor de forma específico para los dispositivos. ¿Hay alguna restricción a los tipos de sistemas o dispositivos que pueden aprobarse según el programa PCI PTS?**

A *La norma PCI PTS no establece factores de forma de dispositivos para permitir a los proveedores desarrollar soluciones innovadoras a fin de satisfacer las necesidades del mercado. Sin embargo, la aprobación de la PTS solo puede obtenerse mediante dispositivos diseñados para la interacción directa con los clientes. Los subcomponentes, como microprocesadores, lectores de tarjetas magnéticas "cans", aceptadores de ICC y otros que están diseñados para integrarse en otro dispositivo que impediría la visualización directa y la interacción del sistema aprobado por el titular de la tarjeta, no pueden aprobarse conforme a los requisitos de PCI PTS.*

P 22 **Julio (actualización) de 2014: los ensambladores de PIN de los puntos de venta sin interfaces de tarjetas pueden aprobarse para su funcionamiento sin conexión cuando se validen para cumplir con un lector de tarjetas externo aprobado por PTS (puede tratarse de un PED aprobado por PTS que funciona como lector de tarjetas externo o un lector de tarjetas seguro). ¿Qué detalles deben incluirse en la lista para dicha configuración?**

A *En la lista, se especificará con qué PED aprobado por PTS SCR el ensamblador de PIN del POS puede realizar la validación de PIN sin conexión. Se incluirá un hipervínculo al PED o SCR aprobado como componente aprobado. Cuando haya varios dispositivos con los que se pueda operar, se enumerarán todos. El uso del dispositivo con un lector no incluido en la lista invalida la aprobación sin conexión.*

P 23 **Octubre (actualización) de 2018: a raíz del descubrimiento del Padding Oracle on Downgraded Legacy Encryption (POODLE), SSL todavía es un protocolo permitido.**

A *Es posible que la SSL siga siendo compatible, pero el proveedor debe documentar (para las versiones 4 y superiores, esto incluye la Política de seguridad publicada en el sitio web de PCI) que es débil de forma inherente y debe eliminarse, salvo que se requiera de forma provisional para facilitar la interoperabilidad como parte de un plan de migración. Para SSL 3, o versiones anteriores de TLS, si son compatibles, deben eliminarse todos los conjuntos de cifrado que usen un solo DES o RC4 . Ambos objetivos pueden alcanzarse mediante la modificación del código fuente para eliminar el soporte de SSL y los conjuntos de cifrado no permitidos y/o la modificación del archivo de configuración. En cualquier caso, la información de la versión del código, incluyendo en caso de que sea aplicable el archivo de configuración modificado, será identificable como parte del firmware aprobado.*

Además, en el caso de todas las nuevas evaluaciones de POI que utilicen el conjunto de protocolos de internet, los dispositivos deben ser compatibles con TLS 1.2 o superior. Además, todas las evaluaciones delta de los dispositivos POI v3, v4, v5 o v6 en las que se ve afectado el módulo de protocolos abiertos deben cumplir con los mismos criterios.

PCI exige que los dispositivos solo sean compatibles con los conjuntos de cifrado para su uso en TLS 1.2 o superior que proporcionen al menos 112 bits de seguridad. Los paquetes de cifrado que componen la AES y otros algoritmos aprobados por NIST son aceptables para su uso. Las conjuntos de cifrado que utilizan la TDEA (3DES) ya no están permitidos debido a las cantidades limitadas de datos que pueden procesarse con una sola clave, es decir, el tamaño de bloque de 64 bits no ofrece una protección adecuada en aplicaciones como el TLS, en las que se cifran grandes cantidades de datos con la misma clave.

P 24 **Mayo (actualización) de 2018: los dispositivos de captura de PIN pueden integrarse físicamente en el mismo dispositivo con otra funcionalidad, como teléfono móvil, capacidades de PDA o terminal de POS. Las configuraciones manuales de los dispositivos de captura de PIN pueden alojar el archivo adjunto (por ejemplo, a través de un trineo, funda o conector de audio) de un teléfono móvil, un PDA o un terminal POS, donde el dispositivo conectado se comunica con el PED. Tal configuración aparece como un solo dispositivo, con interfaces independientes para la captura por parte del empleado y del titular de la tarjeta. ¿Qué consideraciones deben tenerse en cuenta para cualquiera de estas configuraciones?**

A *Para cualquier dispositivo en el que se espera que el titular de la tarjeta utilice la misma interfaz para ingresar el PIN que el empleado usaría en un teléfono, PDA, aplicación de pago, etc., o donde haya varias interfaces en un único dispositivo integrado, el dispositivo integrado debe estar físicamente y reforzado de manera lógica de acuerdo con los requisitos de seguridad de PTS POI.*

En una configuración portátil con un dispositivo adjunto, existe el riesgo de que el titular de la tarjeta capture el PIN en la interfaz equivocada. Además, la interfaz de comunicación entre el PED y el dispositivo adjunto puede dar acceso a este último a las funciones de MSR sin controles criptográficos, lo que permite realizar el "skimming" de los datos de la cuenta de la tarjeta. Por lo tanto, en este modelo de integración:

- *Se evalúan ambos dispositivos y se valida que cumplen con los requisitos del PTS POI; o*
- *El dispositivo PED, que también debe controlar uno o más lectores de tarjetas, debe implementar y validarse conforme al módulo PTS POI SRED. El PED debe hacer cumplir las funciones del SRED para la encriptación de los datos de la tarjeta en todo momento. El PED solo se permite un estado, es decir, para cifrar todos los datos de la cuenta. No puede configurarse para introducir un estado en el que los datos de la cuenta no estén cifrados.*

P 25 **Julio de 2015: los PED portátiles que se conectan a un teléfono móvil, PDA o terminal POS a través de un trineo, funda o conector de audio son necesarios para admitir SRED. ¿Esto se aplica a los PED que se conectan a través de tecnologías inalámbricas, como Bluetooth o wifi, a teléfonos móviles y tabletas?**

A *Sí. Además, para los dispositivos que no implementan el cifrado SRED, la Política de seguridad debe indicar claramente que el sistema no puede implementarse para conectarse a una tableta o teléfono móvil, y que dicho uso infringirá la aprobación del dispositivo. Los sistemas que sí cuentan con la aprobación de SRED deben tener en cuenta que las funciones de SRED deben habilitarse y aplicarse en esos casos de uso para mantener su aprobación.*

P 26 **Mayo (actualización) de 2018: se requieren dispositivos de entrada de PIN que se conecten a un teléfono móvil, PDA o terminal POS a través de un trineo, funda, conector de audio o conexión inalámbrica para admitir SRED. ¿Esto se aplica a los PED que están integrados con otros dispositivos (como una tableta o un teléfono móvil) que aparecen como un solo dispositivo?**

A *Sí. Un dispositivo integrado es aquel en el que dos dispositivos físicos y electrónicos distintos (por ejemplo, un PED y un dispositivo comercial listo para usar, como un teléfono móvil) aparecen como un único dispositivo mediante el uso de plásticos para ocultar la conectividad.*

En tal configuración, existe el riesgo de que el titular de la tarjeta ingrese el PIN en la interfaz equivocada. Además, la interfaz de comunicación entre el PED y el dispositivo integrado puede dar acceso a este último a las funciones del lector de tarjeta sin controles criptográficos, lo que permite realizar el "skimming" de los datos de la cuenta de la tarjeta. Por lo tanto, en este modelo de integración:

- *Se evalúan tanto el PED como el no PED, y se valida que cumplen con los requisitos del PTS POI; o*
- *El PED, que también debe controlar uno o más lectores de tarjetas, debe implementarse y validarse conforme al módulo PTS POI SRED y ser distinto, tanto física como electrónicamente, al sistema no PED (por ejemplo, no es aceptable que el firmware del PED se ejecute dentro del mismo procesador que el firmware no PED). El PED debe hacer cumplir las funciones del SRED para la encriptación de los datos de la tarjeta en todo momento. El PED solo se permite un estado, es decir, para cifrar todos los datos de la cuenta. No puede configurarse para introducir un estado en el que los datos de la cuenta no estén cifrados.*

La Política de seguridad también debe establecer que no se ha evaluado el no PED conforme a la norma PCI PTS y que se requiere una guía sobre seguridad para garantizar el funcionamiento seguro de la solución. Se añadirá una nota adicional al portal en la que se indicará que el no PED no se ha evaluado en el marco del programa PTS.

P 27 **Julio de 2017: para los efectos de la aceptación por parte de PCI, un proyecto de norma es un documento se publicó como borrador para su uso en pruebas (por ejemplo, ISO FDIS) o bien, se publicó como un borrador para recibir comentarios del público (por ejemplo, borradores de NIST).**

A *Sin embargo, el ANSI (X9) no realiza ninguna de las dos opciones mencionadas y debe hacerse una aclaración adicional. Para los efectos de la aceptación por parte de PCI, un proyecto de norma ANSI (X9) es el que ha sido votado a favor por el grupo de trabajo X9 asignado (por ejemplo, X9F1, X9F4 o X9F6). Antes de este punto, los procedimientos de los grupos de trabajo permiten a los miembros publicar documentos en diversas etapas de "borrador", que pueden entrar en conflicto entre sí, y es posible que no reflejen un consenso del grupo de trabajo. La falla de seguridad del algoritmo invalida cualquier norma—en versión borrador o final.*

P 28 **Mayo de 2018: ¿es aceptable que una aplicación de terminal analice los datos de captura, la cual cambia dinámicamente su comportamiento durante el tiempo de ejecución? Por ejemplo, ¿un navegador web o un cliente de correo electrónico puede analizar y mostrar HTML5, Java, JavaScript o cualquier otro lenguaje de programación?**

A *Sí, siempre y cuando el firmware analice, verifique y muestre los datos.*

P 29 Octubre de 2018: ¿hay requisitos mínimos para que la versión de Android se utilice en un dispositivo PTS?

A *Sí, se espera que la versión para Android, como mínimo, esté oficialmente admitida con parches de seguridad. Se rechazarán los informes, incluyendo los deltas, en los que la versión de Android no sea compatible con parches de seguridad regulares. En los casos en que Google no proporcione estos parches, deben documentarse en el informe establecido por PCI las evidencias de parches de seguridad (implementados al menos mensualmente) que suministre el proveedor; las evidencias de lo anterior deben ser la validación del código de actualización por parte del laboratorio para, por lo menos, dos parches anteriores, así como la validación por parte del laboratorio de que estos parches corrigieron las vulnerabilidades conocidas en la versión de Android que se utilice.*

Los proveedores deben tener en cuenta que esto significa que debe considerarse el estado a futuro de los parches de cualquier versión de Android utilizada durante las etapas iniciales de diseño del dispositivo, con el fin de evitar el rechazo inesperado de los dispositivos después de que una versión de Android quede incompatible durante el desarrollo de una solución.

P 30 Octubre de 2018: de acuerdo con DTR: "El eje fundamental para lograr la aprobación del dispositivo es el informe basado en evidencias que demuestren el cumplimiento del dispositivo a través de pruebas sólidas". ¿Cuáles son las expectativas mínimas de pruebas o evidencias de pruebas de resistencia a los dispositivos a los ataques que involucren penetración o modificación física?

A *Aunque la evidencia de corte y/o perforación en el dispositivo (funda exterior, partes interiores) es una actividad de prueba primaria en la mayoría de las evaluaciones, el corte y/o perforación en sí mismo rara vez es suficientes para demostrar una resistencia satisfactoria a todos o cualesquier requisitos de seguridad, donde una ruta de ataque viable tenga elementos de penetración o modificación física. Es necesario que el laboratorio evaluador muestre, además, evidencias sólidas de la resistencia del dispositivo a los ataques físicos que intentan eludir, por ejemplo, interruptores contra manipulaciones, mallas, PCB, circuitos contra manipulaciones, teclados, pantallas, lectores de tarjetas, tableros, etc., y los componentes de estas partes del dispositivo y/o componentes que los conectan.*

Requisito de POI A1

P 1 **¿Qué vulnerabilidades deben tenerse en cuenta para una pantalla táctil?**

A *Si los lados son accesibles, un ataque de superposición utilizando una segunda pantalla táctil clara podría representar un problema. Es necesario verificar que sea segura la conexión o ruta de la pantalla táctil al procesador (y a cualquier dispositivo utilizado para decodificar las señales entre ellas). Los marcos que están alrededor de la pantalla táctil son especialmente peligrosos, porque pueden ocultar el acceso a las áreas de preocupación que se describen anteriormente.*

La API para el firmware y las aplicaciones (si procede) debe examinarse cuidadosamente a fin de determinar las condiciones en que se permite la captura de datos en texto plano. Por ejemplo: no debería ser posible, a menos que en la pantalla del adquirente se muestren los dispositivos con selección dinámica, para que un tercero muestre una imagen (JPEG) que indique "pulse Intro cuando esté listo para la captura de PIN", y luego tenga un teclado de texto sin formato que aparece en la siguiente pantalla. Se garantiza una precaución adicional para los dispositivos de pantalla táctil, porque se pretende que los dispositivos de pantalla táctil sean fáciles de usar, y que puedan ejecutarse muchas aplicaciones diferentes, no autenticadas y no controladas. Esto es especialmente cierto en el caso de los dispositivos destinados a mantenerse, ya que se tiende a considerarlos como un PDA que puede realizar operaciones de débito.

P 2 **En caso de manipulación, el dispositivo debe volverse inmediatamente inoperativo y generar en la eliminación automática e inmediata de cualquier información secreta que pueda almacenarse en el dispositivo, de modo que no pueda recuperarse la información secreta. Las notas de guía establecen que las claves secretas o privadas no deben ponerse a ceros si existen una o ambas de las siguientes condiciones:**

- **Si alguna de estas claves no se pone a ceros, deben existir otros mecanismos para deshabilitar el dispositivo, y estas claves deben estar protegidas de acuerdo con el Requisito A6.**
- **Las claves nunca se utilizan para cifrar o descifrar datos, ni para la autenticación.**

¿Se aplican otras condiciones?

A *Las claves (secretas o privadas) nunca se utilizan para cifrar o descifrar otras claves. Las claves que pueden utilizarse para descargar otras claves para hacer que el dispositivo sea operativo deben ponerse a ceros o inutilizarse para la descarga de nuevas claves; por ejemplo, tanto las KEK simétricas, que se utilizan para la carga de las claves mediante técnicas simétricas, como las claves privadas asociadas a la carga de las claves mediante técnicas asimétricas. El dispositivo debe hacer cumplir que los dispositivos manipulados requieran que se retire del uso para la inspección, la recarga de claves y la nueva puesta en marcha. No basta con utilizar los controles de procedimiento para esto.*

P 3 **Un dispositivo utiliza una clave que se genera aleatoriamente de forma interna en el procesador seguro para proteger otras claves. Esta clave se almacena en formato de texto no cifrado y se protege en un registro dentro del mismo procesador seguro. El procesador seguro se aloja dentro de un área segura del dispositivo. Esta clave se utiliza para cifrar otras claves, que se almacenan cifradas fuera del procesador seguro, es decir, en la memoria flash que también se aloja dentro del área segura del dispositivo. En caso de manipulación, el dispositivo borra esta clave generada internamente, pero deja intactas las otras claves cifradas por esta clave, que ya no pueden utilizarse porque el dispositivo no puede descifrarlas. Conforme al Requisito A1, ¿el dispositivo también debe poner a ceros estas claves cifradas en caso de que se manipulen?**

A *No es necesario que el dispositivo ponga a ceros estas claves cifradas, siempre y cuando se cifren mediante los algoritmos y tamaños de clave apropiados, tal como se define en el Requisito B9.*

P 4 **Mayo (actualización) de 2018: el Requisito A1 establece que un dispositivo utiliza mecanismos de detección de manipulaciones y respuesta que hacen que quede inmediatamente inhabilitado. Si se manipula el dispositivo, ¿puede seguir utilizándose para procesar transacciones con tarjetas de pago que no usan PIN?**

A *Un dispositivo de aceptación de PIN que se manipule debe dejar de procesar inmediatamente todas las transacciones con tarjetas de pago que usen PIN. Solo se admitirá un reinicio, si está implementado, a menos que el dispositivo se retire para su inspección y reparación. Cualquier intervención que permita las transacciones debe requerir que sea presencial en el sitio con el fin de que se valide que NO hubo manipulación del dispositivo, la cual está sujeta a las siguientes condiciones:*

- *Se utilizan técnicas de control dual;*
- *Se establece la responsabilidad y la trazabilidad, incluyendo el registro de las ID de los usuarios, el sello de fecha y hora y las acciones realizadas;*
- *La información confidencial necesaria para la autorización (por ejemplo, contraseñas o códigos de autenticación) se inicializa o se utiliza de manera que se impida la reproducción en el mismo dispositivo o en otro.*

Requisito de POI A2

P 1 **¿Qué vulnerabilidades deben tenerse en cuenta para una pantalla táctil?**

A *Si los lados son accesibles, un ataque de superposición utilizando una segunda pantalla táctil clara podría representar un problema. Es necesario verificar que sea segura la conexión o ruta de la pantalla táctil al procesador (y a cualquier dispositivo utilizado para decodificar las señales entre ellas). Los marcos que están alrededor de la pantalla táctil son especialmente peligrosos, porque pueden ocultar el acceso a las áreas de preocupación que se describen anteriormente.*

La API para el firmware y las aplicaciones (si procede) debe examinarse cuidadosamente a fin de determinar las condiciones en que se permite la captura de datos en texto plano. Por ejemplo, no debería ser posible, a menos que en la pantalla del adquirente se muestren los dispositivos con selección dinámica, para que un tercero muestre una imagen (JPEG) que indique "pulse Intro cuando esté listo para la entrada de PIN" y luego tenga un teclado de texto sin formato que aparece en la siguiente pantalla. Se garantiza una precaución adicional para los dispositivos de pantalla táctil, porque se pretende que los dispositivos de pantalla táctil sean fáciles de usar, y que puedan ejecutarse muchas aplicaciones diferentes, no autenticadas y no controladas. Esto es especialmente cierto en el caso de los dispositivos destinados a mantenerse, ya que se tiende a considerarlos como un PDA que puede realizar operaciones de débito.

Requisito de POI A4

P 1 **Diciembre de 2011: ¿qué requisitos se han establecido para la seguridad de las claves públicas y las funciones de administración de claves en los dispositivos de clase de aprobación SCR?**

A *Las claves públicas deben estar protegidas contra cambios dentro del dispositivo para evitar ataques que pongan en riesgo la seguridad del sistema a través de este vector de ataque. De acuerdo con el Requisito A4, el laboratorio de PCI PTS debe evaluar los dispositivos diseñados para el cumplimiento de las clases de aprobación de SCR, y que dependen de las claves públicas para proporcionar seguridad o autenticación a funciones como actualizaciones de firmware.*

Requisito de POI A5

P 1 **¿Qué normas y métodos se utilizan para medir las "emisiones electromagnéticas"?**

A *Los proveedores deben tener en cuenta que las emisiones de EM pueden suponer un riesgo para los datos del PIN, y deben diseñar dispositivos para mitigar este riesgo. Existen muchos métodos para proteger y minimizar las emisiones de EM. El proveedor debe describir al laboratorio por escrito la manera en que el diseño del dispositivo atiende las emisiones de EM. El laboratorio examinará las evidencias proporcionadas por el proveedor para determinar si fundamentan su afirmación. Las evidencias pueden incluir el propio dispositivo, documentos de diseño, resultados de pruebas de terceros y aprobaciones. Las pruebas se realizarán según sea necesario.*

P 2 **Mayo de 2017: ¿hay alguna situación en la que en el informe de evaluación no tenga que proporcionar un costo de ataque?**

A *Sí, para el Requisito A5 (supervisión durante la captura de PIN), donde las pruebas de cualquier característica externa disponible para la supervisión que satisfaga de manera demostrable los pasos de prueba de DTR aplicables no han encontrado ninguna fuga, debe explicarse por qué cualquier escenario de ataque no puede ser factible para menos de 26 puntos, con un mínimo de 13 para la explotación inicial. En tal situación, no es necesario presentar ningún cálculo formal de ataque.*

Requisito de POI A7

P 1 **Julio de 2017: los evaluadores normalmente utilizan la revisión de código fuente y las pruebas de la implementación para verificar que se implementen los métodos de protección de canal lateral. ¿Cómo debe proceder el evaluador cuando las protecciones están en código creado por el proveedor de chip, y esto solo se proporciona al proveedor de POI como biblioteca y no como código fuente?**

A *El evaluador debe tratar el dispositivo como una caja negra y realizar las pruebas con un alcance más allá de lo que se requeriría de otro modo si el código fuente estuviera disponible para determinar que el dispositivo es resistente al ataque. El apéndice de las Normas de análisis de canal lateral para evaluaciones de PCI-PTS en los Requisitos de prueba derivados proporciona una guía.*

El informe debe estipular claramente qué materiales se proporcionaron para la evaluación y qué se sometió a pruebas específicamente, y los detalles de las contramedidas puestas en práctica e implementadas, incluyendo el código que se revisó. Si los materiales no se proporcionan, deben tratarse como una evaluación de caja negra delineada en el párrafo anterior y notificarse como tal.

Requisitos de POI A8, B15 y C2.4

P 1 **El objetivo de los Requisitos A8, B15 y C2.4 es eliminar la posibilidad de que se ingresen valores de PIN en un momento inadecuado y que el dispositivo los maneje de manera no segura. Una forma de que un proveedor cumpla con los Requisitos A8, B15 o C2,4 es permitir que se capturen únicamente valores de PIN. ¿Sería aceptable permitir la captura de datos numéricos si fueran de tres caracteres o menos y, por lo tanto, no podían representar un valor PIN?**

A *Esto sería aceptable si no hay forma de que un dispositivo acepte la entrada de un valor de PIN en un momento inapropiado. Por ejemplo, no debe ser posible que un dispositivo permita ingresar tres caracteres, cambiar automáticamente los estados sin que el titular de la tarjeta pulse "enter" o alguna otra clave de control y, a continuación, aceptar el resto del valor del PIN.*

P 2 **¿Qué restricciones hay si un dispositivo puede mostrar mensajes no controlados y el teclado se utiliza para ingresar datos que no son PIN?**

A *Los mensajes para la captura de datos que no sean de PIN deben estar bajo el control de la unidad criptográfica y deben ser específicos, de modo que el titular de la tarjeta no ingrese un PIN en un momento inapropiado. Un mensaje no controlado seguido de un aviso ambiguo para los datos que no son PIN podría llevar a un titular de la tarjeta a ingresar su PIN en un momento inapropiado. Por ejemplo, si el dispositivo muestra el mensaje no controlado "Listo para PIN" y luego se le solicitan datos de texto sin formato mientras se muestra "Introducir datos", el titular de la tarjeta puede ingresar su PIN en esta selección dinámica de datos que no es de PIN.*

P 3 **¿Es aceptable que los mensajes no controlados se muestren simultáneamente con indicaciones para la captura de datos?**

A *No. Cualquier texto, incluyendo las imágenes, además de los números y la puntuación, que se muestre junto con una selección dinámica se considera una selección dinámica, y debe cumplir con todos los requisitos que rigen las selecciones dinámicas.*

P 4 **Algunos diseños de dispositivos se ajustan a los mensajes de pantalla controlados por el proveedor o por el adquirente sobre quién tiene la custodia de las claves criptográficas que protegen las actualizaciones de los mensajes. ¿Este dispositivo necesita tener identificadores diferentes?**

A *Si el dispositivo debe aprobarse como un dispositivo con mensajes en pantalla controlados tanto por el adquirente como por el proveedor, debe haber una diferenciación para que los clientes puedan distinguir entre las dos (por ejemplo, diferentes versiones de hardware y/o firmware).*

P 5 **En el caso de los dispositivos que tienen mensajes controlados por el adquirente, ¿se requiere el uso de un dispositivo seguro criptográfico a fin de implementar el control dual necesario para manejar esos mensajes?**

A *El control dual debe aplicarse mediante un SCD, que puede ser el propio PED u otro dispositivo. Si un SCD que no sea el PED aplica el control dual, el proveedor debe proporcionar el SCD a terceros o describir cómo debe utilizarse un SCD para cumplir con el Requisito B15. La descripción debe incluir un ejemplo de un SCD específico que pueda comprarse y utilizarse para cumplir con el Requisito B16. El PED debe tener una API compatible con el SCD. La solución completa debe desarrollarse en su totalidad. No es aceptable dar instrucciones detalladas que requieran que los usuarios creen parte de la solución.*

P 6 **Diciembre (actualización) de 2017: para los PED diseñados con múltiples interfaces de aceptación de datos, donde hay un teclado físico dedicado para la entrada de PIN (y otros datos confidenciales), y la otra interfaz es una interfaz táctil que no está diseñada para aceptar una entrada de datos confidenciales, ¿qué controles se requieren para la segunda interfaz?**

A *En este tipo de diseño, deben aplicarse los siguientes controles en la interfaz "no sensible", además de la restricción de que las aplicaciones no deben solicitar la captura de datos confidenciales:*

- *El firmware debe diseñarse de modo que no se puedan ingresar datos confidenciales en la interfaz "no sensible".*
- *Si las coordenadas táctiles x o y se envían a las aplicaciones autenticadas del dispositivo, el proveedor debe proporcionar guía a los programadores de aplicaciones para que nunca las reenvíen. Además, el proveedor debe revisar todas las aplicaciones y NO firmarlas ni autenticarlas si están escritas para enviar coordenadas táctiles, con lo que no permite que se carguen; o*
- *Si el PED autentica el punto de conexión que reciben las coordenadas x o y, y si el enlace de comunicación entre esas instancias se cifra de forma segura (por ejemplo, mediante un túnel TLS v1.2), el dispositivo puede proporcionar coordenadas táctiles x o y solo a aplicaciones o servidores que se hayan sido autenticado con el dispositivo.*

Requisito de POI A8

P 1 ¿El cálculo de la posibilidad de ataque de 18 por dispositivo puede incluir el costo de los kits de desarrollo que proporcionan información de programación de aplicaciones?

A *No. El dispositivo debe incluir protecciones que requieren que un atacante logre una posibilidad de ataque de, por lo menos, 18 para poder vencerlos. Los controles administrativos de la información de programación de aplicaciones no son adecuados para cumplir con este requisito.*

P 2 Los dispositivos de pantalla táctil ofrecen múltiples posibilidades para la entrada de datos: disposición tradicional de teclado de PIN, disposición QWERTY, captura de firmas, reconocimiento de escritura a mano, etc. ¿Se aplica el Requisito A6 a todos estos métodos de entrada de datos o solo al ensamblador de PIN tradicional?

A *El Requisito A6 se aplica a todos los métodos de entrada de datos que puede utilizar el titular de la tarjeta para ingresar su PIN, incluyendo el diseño QWERTY, la captura de firmas y el reconocimiento de escritura a mano.*

Requisito de POI A9

P 1 El Requisito A9 estipula que el dispositivo debe proporcionar un medio para impedir que puedan visualizarse los valores PIN mientras los ingresa el titular de la tarjeta. ¿Qué métodos son aceptables?

A *Los requisitos de seguridad de POI establecen varias opciones que pueden utilizarse por separado o en combinación para proporcionar privacidad durante la entrada de PIN. Estas opciones son:*

- *Una barrera de protección física (privacidad). Tenga en cuenta que, en caso de que el escudo de privacidad pueda extraerse, el dispositivo debe incluir una guía del usuario que establece que el escudo de privacidad debe utilizarse para cumplir con la norma ISO 9564. Opcionalmente, la guía del usuario también puede hacer referencia a los requisitos del dispositivo de PCI;*
- *Un diseño que permita que el titular de la tarjeta pueda ocultarlo con el cuerpo para evitar visualizar el PIN durante la captura del mismo; por ejemplo, un dispositivo portátil;*
- *Un ángulo de visualización limitado (por ejemplo, un filtro de polarización o un ensamblador de PIN empotrado);*
- *Una carcasa que forme parte del cajero automático o del quiosco, la mano o el cuerpo del titular de la tarjeta (solo se aplica a dispositivos portátiles); y*
- *El entorno del dispositivo instalado.*

P 2 **Septiembre (actualización) de 2016: ¿existe algún impacto en la aprobación del dispositivo si no se utiliza el método de privacidad evaluado por un laboratorio?**

A *Con frecuencia, las empresas que colocan los dispositivos excusan que los mecanismos de protección de la privacidad pueden resultar voluminosos u molestos, dificultar ver la pantalla del dispositivo o, con usuarios menos diestros, interferir con el pago con tarjeta y la captura de PIN. Sin embargo, a fin de mantener la aprobación del dispositivo, y cualquier protección de responsabilidad relacionada para el riesgo atribuible al uso de dicho dispositivo, se requiere que el dispositivo cumpla con los requisitos de protección de la privacidad evaluados por el laboratorio y en los que se basó la aprobación. Los dispositivos implementados que no utilizan los requisitos de protección de la privacidad evaluados por el laboratorio de pruebas ya no se consideran aprobados. Esto debe informarse en la política de seguridad del dispositivo.*

P 3 **Septiembre de 2016: los proveedores deben proporcionar un escudo de privacidad durante la captura del PIN del titular de la tarjeta o, alternativamente, el proveedor puede utilizar criterios de escudo de privacidad menos restrictivos siempre y cuando establezca reglas y ofrezca una guía sobre cómo impedir su visualización desde el entorno en el que se instala el dispositivo. ¿Esto afecta la divulgación de la política de seguridad?**

A *Sí. La política de seguridad debe estipular las normas y guía conforme a las que el dispositivo se evaluó en cuanto a cómo debe impedirse la visualización desde el entorno en el que el dispositivo está instalado. La política también debe revelar que, si la implementación no utiliza estas consideraciones evaluadas por el laboratorio y en las que se basó la aprobación, se invalidará la aprobación del dispositivo.*

Si el dispositivo incluye un escudo de privacidad extraíble, la política de seguridad debe establecer esa implementación sin que el escudo invalide la aprobación, salvo que el dispositivo se implemente de acuerdo con las instrucciones de la política de seguridad validada por el laboratorio para implementar el dispositivo con protecciones proporcionadas por el entorno en el que está instalado. La política también debe incluir que, si la implementación no utiliza estas consideraciones evaluadas por el laboratorio y en las que la aprobación se basó, se invalidará la aprobación del dispositivo.

Requisito de POI A10

P 1 **Septiembre de 2013: por ejemplo, si un dispositivo recibe datos de cuentas que se ingresan con la clave en otro dispositivo, ¿puede validarse un dispositivo como SRED si recibe datos de cuentas que se ingresan en un módulo o dispositivo no integrado?**

A *El módulo o dispositivo externo donde se capturan los datos de la cuenta puede recibir la aprobación de SRED si se evalúa junto con el dispositivo POI. La aprobación de SRED dependería de que ambos dispositivos cumplan con todos los requisitos de SRED aplicables, incluyendo la protección de claves criptográficas. Deben cifrarse los datos de cuentas (tal como se definen en el glosario de los* Requisitos de seguridad de PTS POI de PCI *) que atraviesan la ruta de comunicación desde el punto de captura externo de acuerdo con estos requisitos. Ambos dispositivos formarían parte de la lista de aprobación, y la sustitución del dispositivo externo por otro que no esté validado en el SRED invalida la aprobación otorgada del SRED como función.*

Si el dispositivo externo no puede cumplir con los requisitos SRED, el dispositivo principal, aunque proteja de otro modo los datos de cuentas conforme a SRED, no puede recibir la designación SRED si es capaz de recibir datos de cuentas de dicho dispositivo, independientemente de si dichos datos se reciben cifrados. En este caso, para que el dispositivo principal reciba la aprobación SRED, el firmware del dispositivo principal no debe ser compatible con la recepción de los datos de cuentas capturados de manera externa.

Requisito de POI A11

P 1 **Noviembre de 2012: cuando se utiliza una lista blanca para controlar si los datos PAN salen del dispositivo en texto plano o en texto cifrado, ¿la actualización de la lista blanca tiene que estar bajo el control directo del proveedor?**

A *No, el proveedor puede proporcionar al adquirente los mecanismos para controlar directamente la actualización de las listas blancas de manera coherente con los mensajes de pantalla controlados por el adquirente,—es decir, usar técnicas de control dual y disposiciones para la auditabilidad y el registro.*

Alternativamente, el proveedor podrá entregar documentación del usuario en la que se establezca la administración de las claves criptográficas siguiendo estos principios e implementando el uso de un dispositivo criptográfico seguro para la administración de estas claves. El proceso existe del cliente al servidor del dispositivo, pero este debe seguir proporcionando la aplicación, es decir, validar el MAC o la firma digital.

Requisito de POI A13

P 1 **¿Qué significa "suficiente espacio para guardar un 'error' que permite revelar el PIN"?**

A *No se permite el espacio accesible a través de la ranura de la tarjeta ICC lo suficientemente grande para ocultar un error que revele el PIN. Tal error podría utilizar la tecnología ICC. Por lo tanto, no debe haber espacio accesible a través de la ranura de la tarjeta lo suficientemente grande como para ocultar un chip ICC y una batería pequeña.*

P 2 ¿Qué volumen de espacio está permitido conforme al Requisito A13?

A *El objetivo del Requisito A13 es evitar que se inserte un error de revelación del PIN en el dispositivo a través de la ranura de la tarjeta. El volumen del espacio accesible a través de la ranura para tarjetas que podría utilizar un atacante puede variar según la geometría del espacio y los métodos de ataque. Por este motivo, el requisito no prohíbe un volumen específico. Más bien, debe considerarse la viabilidad de la colocación eficaz de errores al evaluar el cumplimiento del Requisito A14. Algunos ejemplos de estas consideraciones:*

- *Los puntos de contacto deben estar presentes para conectar el error.*
- *El error y los cables no deben obstruir el funcionamiento normal.*
- *La colocación del error no debe generar pruebas de manipulación que notaría un titular de la tarjeta típico.*

P 3 Mayo de 2018: la nueva clase de aprobación del SCRP aumenta el nivel de protección requerido para la interfaz de E/S del ICC a 26 puntos. ¿Por qué se exige esto si otras clases de aprobación siguen permitiendo que se considere que un dispositivo cumple al presentar un nivel de 20 puntos de protección?

A *La intención de la clase de aprobación del SCRP es asegurar que los datos de la tarjeta del cliente estén protegidos y encriptados de forma segura antes de que se envíen a través del dispositivo de entorno COTS a los sistemas de backend para el procesamiento de pagos. Esta es una parte importante de la seguridad general de la solución de sistema PIN on COTS (SPoC) Entrada de PIN basada en software en COTS, y ayuda a prevenir los ataques de correlación y a reducir la amenaza de que el PIN del dispositivo COTS esté en riesgo. Dado que la protección de la señal de E/S de la CCI requiere la protección desde la interfaz física hasta la tarjeta del cliente y el procesador de seguridad que realiza la encriptación de estos datos, la exigencia de un aumento de los mínimos de puntos de ataque para ello tiene, por lo tanto, el efecto de aumentar las protecciones generales requeridas en el SCRP en su conjunto—que, a su vez, tiene un efecto de reducción del riesgo de robo de PIN en el dispositivo COTS.*

Es posible que otras clases de aprobación en las que se aceptan tarjetas ICC no procesen los PIN o bien, se les exija que cumplan con otros cálculos de costos de ataque y mínimos dentro de los requisitos de PCI PTS, y por lo tanto, no dependen tanto de la separación de los datos de tarjetas de cliente y PIN. Por eso, los puntos de ataque pueden permanecer en 20 para esos otros casos de uso.

Requisito de POI A14

P 1 ¿El Requisito D2 tiene el objetivo de aplicarse a la apertura del lector de ICC o a todo el lector?

A *El Requisito D2 se establece en el entendimiento de que la abertura (ranura) es un posible punto de ataque para insertar un mecanismo de manipulación.*

P 2 Algunos diseños de dispositivos incluyen componentes (por ejemplo, escudo de privacidad) que están cerca de la ranura de la tarjeta IC y pueden utilizarse para ocultar un cable. ¿Qué criterios se utilizan para determinar el cumplimiento cuando están presentes esos componentes?

A *Se considera que el diseño cumple con el Requisito A14 si una parte del cable es visible entre la ranura y el componente de ocultamiento.*

Requisito de POI B1

P 1 **Si un dispositivo utiliza firmware en el cabezal de lectura de MSR para cifrar los datos de cuentas, ¿ese firmware está sujeto a la verificación de autenticidad conforme a la definición del Requisito B1?**

A *No. La comprobación de la autenticidad, conforme a la definición del Requisito B1, está destinada a la administración del firmware que interviene directa o indirectamente en la protección de los PIN del titular de la tarjeta, tal como se define en los diversos requisitos de seguridad. Sin embargo, el firmware del cabezal de lectura debe estar diseñado de tal manera que no pueda actualizarse.*

P 2 **¿En qué circunstancias un dispositivo no puede utilizar la comprobación de la autenticidad al realizar una prueba automática de su firmware?**

A *Un dispositivo no requiere verificación de la autenticidad cuando realiza pruebas automáticas a su firmware si (todos aplican):*

- *La verificación de autenticidad del firmware se realiza, ya sea internamente y conforme al Requisito B2 o externamente mediante los procedimientos adecuados dentro de un entorno seguro bajo el control del proveedor, siempre que el firmware se establece en esa área segura;* ***y***
- *La actividad de modificación o reemplazo del firmware o de sus componentes de manera deliberada para obtener acceso a información confidencial (acceso al dispositivo de memoria) debe abordarse como un escenario de ataque conforme a los Requisitos A1, A4 y A6 y cumplir con las respectivas posibilidades de ataque;* ***y***
- *Se realiza una verificación periódica de integridad de acuerdo con el Requisito B1 para el firmware, lo que garantiza que se detecten cambios aleatorios; si no se realiza la autenticidad criptográfica, la verificación de integridad debe hacerse de manera criptográfica. Aunque puede utilizarse un algoritmo de clave secreta, como un hash con clave, no es necesario para cumplir con los criterios de integridad.*

Estas condiciones aplican independientemente de cualquier propiedad de la memoria del dispositivo que no se pueda reconfigurar.

Cuando el firmware se autentica de manera externa, el nivel de seguridad deberá ser el mismo que el de las instalaciones de inyección de claves.

Requisito de POI B2

P 1 **¿Qué partes pueden poseer las claves utilizadas para la autenticación criptográfica de las actualizaciones del firmware?**

A *El firmware es responsabilidad del proveedor del dispositivo y, como tal, las claves criptográficas que lo autentican dentro del dispositivo deben estar únicamente en su poder o en el de su agente designado.*

P 2 **Las actualizaciones de firmware deben autenticarse criptográficamente; si la autenticación falla, se rechazan y eliminan. ¿Hay algún caso en el que el firmware pueda actualizarse sin autenticación?**

A *Algunos chipsets no están diseñados para actualizaciones de firmware, sino únicamente para admitir el reemplazo del firmware. La eliminación del firmware y de las claves criptográficas durante el reemplazo no permite que se realice la autenticación del nuevo firmware.*

En esos casos, es aceptable actualizar el firmware sin autenticación si el proceso requiere que el dispositivo se devuelva a las instalaciones del proveedor, y tiene como resultado la puesta a ceros segura de todas las claves secretas y privadas contenidas en el dispositivo.

P 3 **Diciembre de 2011: si un dispositivo admite actualizaciones de firmware, debe autenticar criptográficamente el firmware; si el firmware no se confirma, su actualización debe rechazarse y eliminarse. Si se conserva una copia de seguridad protegida del código autenticado, ¿un dispositivo puede cargar por completo un firmware nuevo antes de comprobar su autenticidad y sobrescribir su copia principal del código autenticado?**

A *Sí, siempre y cuando se cumpla lo siguiente:*

- *El nuevo código se autentica criptográficamente antes de la ejecución.*

  Si el nuevo código falla en la autenticación, la copia de seguridad del código se autentica criptográficamente; si lo hace de manera satisfactoria, el dispositivo se inicia desde la copia de seguridad y esta se utiliza para sobrescribir el nuevo código que falló en la autenticación.

- *Si ambas versiones de firmware fallan en la autenticación, el dispositivo falla de forma segura.*

P 4 **Febrero de 2017: si el dispositivo utiliza firmas digitales para autenticar las actualizaciones del firmware (conforme al Requisito B2), ¿requiere utilizar un protocolo seguro para cumplir con el Requisito B22?**

A *El Requisito B2 estipula que el firmware cargado en el dispositivo debe autenticarse independientemente de cómo se envíe el archivo al dispositivo.*

El Requisito B2 garantiza que la plataforma de administración entregue los archivos al dispositivo de forma segura y que la interfaz no pueda utilizarse como un vector de ataque en el dispositivo.

- *Para el acceso remoto, es decir, los archivos se entregan al dispositivo a través de una red privada o pública, se requiere el uso de un protocolo de seguridad y debe validarse.*

- *Para el acceso manual,es decir, cuando el operador tiene control físico de la terminal y los archivos, y los archivos no se entregan a través de una red, el dispositivo debe garantizar que no pueda explotarse la interfaz (por ejemplo, mediante la restricción del acceso o funcionalidad en la interfaz, requerimiento de derechos de administración, técnicas de autenticación criptográfica, etc.).*

El Requisito B22 establece que es solo para acceso remoto y no incluye un elemento manual; se requeriría un protocolo de seguridad para garantizar que no se explote la interfaz.

Requisito de POI B2.2

P 1 **Marzo de 2011: las aplicaciones autenticadas pueden crearse con el proveedor de POI o terceros. Las aplicaciones deberán desarrollarse mediante técnicas que cumplan con PA-DSS y autenticarse criptográficamente mediante el POI. ¿Hay alguna otra consideración?**

A *Sí. La técnica utilizada para administrar el mecanismo de autenticación (por ejemplo, las firmas digitales) debe utilizar un SCD y técnicas de control dual. En el caso de terceros, el proveedor del dispositivo debe proporcionar el SCD a los terceros o describir cómo debe utilizarse un SCD para cumplir con el Requisito B7. La descripción debe incluir un ejemplo de un SCD específico y actual que pueda adquirirse y utilizarse para cumplir con el Requisito B5. El POI debe tener una API que sea compatible con el SCD. La solución completa debe desarrollarse en su totalidad. No es aceptable proporcionar instrucciones detalladas que exijan que los usuarios desarrollen parte de la solución.*

Requisito de POI B4

P 1 **El Requisito B4 establece que un PIN debe cifrarse inmediatamente. Por lo general, esto significa que el procesador seguro forma y cifra el bloqueo de PIN antes de realizar cualquier otra operación. Sin embargo, algunos diseños de dispositivos colocan un microprocesador entre el teclado y el procesador seguro. De haberlas, ¿en qué condiciones se permitiría tal diseño?**

A *Se considera que cumple tal diseño si el microprocesador, el procesador seguro y la ruta entre ellos están completamente dentro del límite protector del dispositivo. Este límite se establece a través del método elegido para cumplir con el Requisito A1.*

Un método alternativo para cumplir con los requisitos sería que el microprocesador cifre inmediatamente el PIN antes de transferirlo al procesador seguro, que luego lo descifraría y crearía el bloque de PIN cifrado. Obsérvese que, en este tipo de diseño, el software del microprocesador para cifrar los datos del PIN se utiliza para cumplir los requisitos de la PCI. Por lo tanto, este software debe considerarse como "firmware" según los requisitos de PCI. Por lo tanto, los Requisitos B3 y B4 se aplicarían a este firmware.

P 2 **Una práctica habitual es cifrar los ensambladores de PIN utilizados en cajeros automáticos para admitir el uso de un comando para iniciar la entrada de PIN y otro comando para cifrar el PIN. ¿Es esto aceptable conforme al Requisito B4?**

A *Sí. Es aceptable que un EPP permita que un comando inicie la entrada de PIN y un segundo comando, el su cifrado. Sin embargo, el comando de cifrado no puede utilizarse para cifrar el PIN varias veces y generarlo desde el EPP con diferentes claves criptográficas o para generar el PIN en texto plano. Además, el valor de PIN de texto plano solo debe existir en la memoria protegida contra manipulaciones o equivalente.*

P 3 **Septiembre de 2012: los dispositivos pueden admitir el cifrado del PIN varias veces como parte de una serie de transacciones. El Requisito B4 estipula que los cifrados deben utilizar la misma clave de cifrado para esta serie. ¿Puede cifrarse la serie de transacciones mediante claves si la clave actual es una derivación de una clave predecesora?**

A *El propósito del requisito es evitar que un atacante utilice la clave autorizada para enviar la transacción en línea para su autorización y otra clave para registrar la transacción para su posterior recuperación. En ese sentido, puede utilizarse una metodología UKPT para la serie de transacciones, mediante la cual las claves son parte de la misma serie y toda la jerarquía se protege de la misma manera, y no es factible insertar una clave no autorizada en el diseño.*

P 4 **Abril de 2013: el Requisito B4 exige que los PIN en línea se cifren inmediatamente después de que se complete la entrada de PIN. Además, se estipula que los PIN en texto plano no deben existir durante más de un minuto a partir de que finalice la entrada de PIN del titular de la tarjeta. En todos los casos, el PIN en texto plano debe borrarse antes de que los mecanismos de detección de manipulaciones puedan desactivarse con los métodos de ataque descritos en A1. ¿Hay alguna circunstancia en la que un PIN en texto plano pueda existir durante más de un minuto?**

A *Algunos cajeros automáticos han implementado tecnologías de depósitos inteligentes para mejorar la experiencia del cliente. Como resultado, algunas transacciones de depósito tardan más de un minuto, lo cual redunda en que el PIN se libere del búfer después de un minuto y el titular de la tarjeta tenga que iniciar la transacción de nuevo y, en algunos casos, no pueda completar la transacción. En esos casos, las aplicaciones de los cajeros automáticos requieren una modificación para solicitar que vuelva a ingresarse el PIN si una transacción se prolonga más allá del periodo de vencimiento, en lugar de exigir que se reinicie toda la transacción.*

Con el fin de ofrecer un tiempo suficiente para la modificación de esas aplicaciones, PCI dará tres años a partir de la publicación de estas preguntas frecuentes para que se modifiquen esas aplicaciones. Durante este periodo, el PIN no cifrado puede permanecer hasta cinco minutos en el búfer. Sin embargo, debe permanecer protegido de cualquier riesgo mediante los métodos de ataque establecidos en el Requisito A1, y el laboratorio de pruebas deberá tener en cuenta la falta de un cifrado oportuno al diseñar los ataques.

Este aplazamiento solo se aplica a la codificación de los ensambladores de PIN diseñados y usados para cajeros automáticos.

Requisito de POI B5

P 1 **Durante la carga de la clave, ¿es aceptable que los componentes de la clave XOR se utilicen para cumplir con el Requisito B5 de autenticación?**

A *La compuerta XOR de los componentes clave por sí sola no es suficiente para una autenticación. Se requiere algún tipo de autenticación de los usuarios que utilizan la función o la autenticación del comando de carga de claves.*

P 2 **Mayo 2018 (actualización): ¿en qué circunstancias se permite la entrada de claves a través del teclado del dispositivo?**

A *Las claves secretas de un componente único en texto plano no pueden ingresarse en el dispositivo mediante el teclado. Los componentes de una clave de texto plano pueden ingresarse a través del teclado de acuerdo con la norma ISO 11568-2. Las claves cifradas también pueden ingresarse a través del teclado. La entrada de los componentes de las claves o las claves cifradas debe estar restringida a las personas autorizadas. Las funciones utilizadas para ingresar las teclas solo deben estar disponibles cuando el dispositivo se encuentra en un estado confidencial. El acceso a las funciones confidenciales debe restringirse mediante el uso de contraseñas o códigos de autenticación u otros datos secretos.*

P 3 **¿Los menús de mantenimiento que prestan servicios, como el ajuste del contrato de LCD, pruebas automáticas, mantenimiento de la impresora y pruebas clave, constituyen un "servicio confidencial"?**

A *Si los servicios prestados en estas funciones normalmente no permitidas no afectan la seguridad de la terminal o a los datos del titular de la tarjeta, no se consideran servicios confidenciales. Solo aquellos que podrían poner en riesgo la seguridad de la terminal son servicios confidenciales.*

P 4 **En el caso de los dispositivos que requieren datos de autenticación para acceder a funciones confidenciales, y dichos datos son estáticos, ¿pueden enviarse los datos de autenticación con el dispositivo?**

A *Los datos de autenticación pueden enviarse con el dispositivo solo cuando estos se encuentran en un embalaje a prueba de manipulación, como el uso de correos con PIN. De lo contrario, deben utilizarse canales de comunicación independientes, con destinatarios predefinidos.*

P 5 **Marzo de 2011: las claves privadas o secretas de texto plano y sus componentes pueden insertarse en un PIN mediante un cargador de claves (que tiene que ser algún tipo de dispositivo seguro criptográfico). ¿Existen restricciones en la carga de claves a través de esta metodología?**

A *Sí, la carga de claves privadas o secretas de texto plano y sus componentes que utilizan un dispositivo de cargador de claves está restringida para proteger las instalaciones de carga de claves. Los dispositivos que se dejan sin vigilancia y que están implementados en el campo tendrán una carga de clave privada o secreta de texto plano, la cual está restringida a los componentes de la clave introducidos a través del teclado numérico del ensamblador de PIN. Si están cifradas, estas claves pueden cargarse a través de otra interfaz, como un puerto serie o USB.*

P 6 **Diciembre de 2011: es posible que los dispositivos tengan funciones para poner a ceros las claves secretas y privadas en el dispositivo. ¿Estas funciones se consideran servicios confidenciales que requieren autenticación?**

A *Sí, la puesta a ceros de claves secretas o privadas de manera intencional en un evento no manipulable consiste en la ejecución de funciones que no están disponibles durante el uso normal. Esto requiere una autenticación coherente con las implementaciones de otros servicios confidenciales, como el uso de PIN o frases de contraseña. Si se implementa, el dispositivo debe obligar a cambiar los valores de autenticación de los valores predeterminados en la configuración del dispositivo. El mecanismo de autenticación puede utilizar de manera opcional técnicas de control dual.*

P 7 **Junio (actualización) de 2015: es posible que los dispositivos tengan funciones para poner a ceros las claves secretas y privadas en el dispositivo. Esta funcionalidad se considera un servicio confidencial que requiere autenticación. En algunos casos, hay un efecto del cliente al servidor en el que los cambios de software deben producirse en los puntos de interfaces, como plataformas de cajeros automáticos, aplicaciones, conmutadores y hosts que interactúan con los EPP. ¿Hay alguna dispensa de este requisito?**

A *Todos los dispositivos que implementen esta funcionalidad deben cumplir con los requisitos. Sin embargo, el dispositivo puede hacerlo mediante la implementación de un nuevo comando de eliminación autenticado en el conjunto de comandos del EPP, además de los comandos actuales. Esto debe codificarse como una opción de uno u otro modo, de manera que ambos métodos no estén disponibles al mismo tiempo. Una vez que se elige la opción de autenticación, se bloquearían permanentemente los comandos no autenticados.*

En todos los casos, debe existir un periodo límite de validez para forzar la implementación de los cambios de software del cliente al servidor dentro de un tiempo establecido. PCI permitirá que se modifiquen tres años a partir de la publicación de estas preguntas frecuentes para esas aplicaciones. Este aplazamiento solo se aplica a la codificación de los ensambladores de PIN diseñados y usados para cajeros automáticos.

A partir del 1 de enero de 2017, todos los EPP recientemente aprobados solo deben admitir la capacidad de eliminación autenticada. No es necesario que los EPP aprobados antes de enero de 2017 con capacidad de eliminación no autenticada se actualicen a la capacidad de eliminación autenticada para mantener el cumplimiento de la PCI.

Requisito de POI B7

P 1 **Enero de 2015: es un requisito de DTR B21 que un POI genere el número impredecible (UN) de EMV para cualquier transacción basada en PIN mediante el RNG interno, conforme a las pruebas establecidas en el Requisito B7. ¿También se requieren transacciones no basadas en PIN para generar el UN a partir del RNG del POI?**

Sí, debe utilizarse el RNG del POI para generar todos los valores aleatorios e impredecibles que se emplean para la seguridad de los datos de la tarjeta y las transacciones con PIN. Cuando se utiliza el POI para generar el UN de EMV, debe emplearse el RNG del POI, independientemente del método de verificación del titular de la tarjeta implementado para esa transacción. Tenga en cuenta que el proceso de generación de UN de EMV puede incorporar otros datos, como registros internos y datos de transacciones (vea, por ejemplo, el algoritmo de generación de UN de EMV en http://www.emvco.com.

Requisito de POI B9

P 1 **¿Es aceptable que un dispositivo tenga la capacidad de utilizar las claves maestras tanto como claves de cifrado para la clave de sesión como claves fijas (es decir, que la clave maestra pueda utilizarse para cifrar bloques de PIN y para descifrar claves de sesión)?**

A *No. Una clave debe utilizarse para un solo propósito como se establece en las normas ANSI X9.24 e ISO 11568.*

P 2 **¿Es aceptable utilizar la misma técnica de autenticación para cargar claves criptográficas y firmware?**

A *La técnica puede ser la misma, pero las preguntas secretas para la autenticación deben ser diferentes. Por ejemplo, si se utilizan firmas de RSA, la clave privada de RSA para firmar claves criptográficas para cargar debe ser diferente de la clave privada utilizada para firmar firmware.*

P 3 **¿Es aceptable el cifrado de modo ECB de TDES para las claves de sesión cuando se utiliza la técnica de clave maestra o clave de sesión?**

A *Sí. El modo TDES ECB puede usarse para encriptar las claves de sesión.*

P 4 **¿Es aceptable cargar componentes de clave TDES de 128 bits de doble longitud en un dispositivo en valores de bits más pequeños (por ejemplo, dos partes de 64 bits que conserva el custodio de claves 1 y dos partes de 64 bits que conserva el custodio de claves 2)?**

A *Sí, siempre y cuando las claves TDES criptográficas de 128 bits (y los componentes de las claves) se generen y administren como claves TDES de 128 bits de doble longitud completa durante todo su ciclo de vida de acuerdo con las normas ANSI X9.24 e ISO 11568.*

Por ejemplo, sería aceptable generar un componente de clave TDES de 128 bits de longitud completa, pero debe cargarse en el dispositivo como dos mitades de componentes de 64 bits.

No sería aceptable generar claves de 64 bits o componentes de claves por separado y luego concatenarlas para su uso como clave de doble longitud después de la generación.

Si se utilizan valores de comprobación de claves para garantizar la integridad de estas, deben calcularse sobre la totalidad del componente de clave de 128 bits o la clave de 128 bits

resultante, pero nunca sobre una parte de la clave o su componente. Además, la clave resultante dentro del dispositivo debe recombinarse de acuerdo con los requisitos de PCI y las normas ANSI/ISO. De manera similar, en el caso de las claves de triple longitud, para calcular los valores de comprobación, debe utilizarse el componente completo de clave de 192 bits o la clave de 192 bits resultante.

P 5 ¿En qué condiciones es aceptable que un dispositivo permita cargar claves criptográficas de texto plano de componente único a través del teclado?

A *En ninguna. Un dispositivo no debe aceptar la entrada de claves criptográficas de texto plano de un solo componente a través del teclado. Los componentes de clave de longitud completa y las claves cifradas pueden cargarse a través del teclado si se cumplen con los requisitos de funciones confidenciales* ***(PCI B5, B6)****.*

P 6 ISO 11568-2 *Claves simétricas, su manejo clave y ciclo de vida* y ANSI X9.24-1 *Administración de claves simétricas, servicios financieros personales Parte 1: uso de técnicas simétricas* estipulan que cualquier clave que exista en un dispositivo de origen de transacciones no existirá en ningún otro dispositivo de ese tipo. ¿Se aplica eso a todas las claves secretas y privadas contenidas en un dispositivo?

A *El objetivo del requisito es que el riesgo de una clave en un dispositivo que origina una transacción (por ejemplo, un dispositivo EPP o POS) no afecte la seguridad de otro dispositivo similar. En este sentido, toda clave privada o secreta presente o utilizada de otro modo en un dispositivo de origen de transacciones debe ser exclusiva de ese dispositivo, salvo por casualidad. Esto incluye las claves utilizadas para la codificación del PIN, la validación del firmware, el control de los mensajes de pantalla o la protección de cualquiera de esas mismas claves durante la carga o el almacenamiento al/dentro del dispositivo. Tenga en cuenta que cada una de estas funciones requiere su propia clave única.*

Este requisito se aplica tanto a las claves originadas por el proveedor como por el adquirente o claves controladas. Esto no incluye las claves públicas presentes o utilizadas por el dispositivo.

P 7 Los dispositivos pueden admitir la carga remota de las claves secretas del adquirente mediante técnicas asimétricas. Todo protocolo de carga de claves a distancia de ese tipo debe establecer un mecanismo para reducir al mínimo la probabilidad de que se produzcan ataques de tipo intermediario" en los que un dispositivo pueda engañarse para que se comunique con un host ilegítimo. Un mecanismo común es "enlazar" el host al dispositivo para que no acepte comunicaciones que no estén firmadas digitalmente por el host legítimo y autenticadas por el dispositivo. Existen diferentes situaciones en las que puede ser necesario cambiar de host y/o pares de claves asimétricas de host. Cuando se desbloquean los pares de claves de un host del dispositivo, lo que puede hacerse manualmente en el dispositivo o de manera remota mediante un comando firmado y autenticado digitalmente, ¿hay alguna disposición especial establecida?

A *Una vez recibida una instrucción válida para desvincular un par de claves de host de un dispositivo, este debe poner a ceros las claves secretas de cualquier entidad adquirente. La mayoría de las situaciones en las que es necesario desvincular un host son consecuencia de un cambio en la entidad adquirente. Sin embargo, en todos los casos, el dispositivo debe inicializarse con nuevas claves secretas para la entidad adquirente antes de ponerlo en servicio de nuevo.*

P 8 **La metodología TR-31 define tres claves: clave de protección de bloqueo de claves (KBPK), clave de cifrado de bloque de claves (KBEK) y clave MAC de bloqueo de claves (KBMK). La KBPK se utiliza para calcular la KBEK y la KBMK. ¿Puede usarse la KBPK con cualquier otro propósito?**

A *No, para cumplir con el requisito de que una clave se utilice con un solo propósito, tal como se define en la norma ANSI X9.24, la clave de protección del bloque de la clave solo se utiliza con el propósito de calcular la KBEK y la KBMK. La KBPK solo se utiliza para generar la KBEK y la clave KBMK; no se utiliza ninguna otra clave con este propósito.*

P 9 **Debe utilizarse TR-31 o una metodología equivalente siempre que se descargue una clave simétrica desde un host remoto cifrado por una clave simétrica compartida. ¿Existen otras circunstancias en las que se aplica o no se aplica TR-31 o una metodología equivalente?**

A *Los dispositivos deben admitir la metodología TR-31 o una equivalente para la carga de claves siempre que otra clave simétrica cargue una clave simétrica. Esto aplica tanto si las claves simétricas se cargan manualmente (es decir, a través del teclado), utilizando un dispositivo de inyección de claves o desde un host remoto. No aplica cuando las claves simétricas de texto simple o sus componentes se cargan mediante técnicas estándar de control dual.*

P 10 **En apoyo a la conversión de los dispositivos implementados para el uso de la metodología TR-31, una clave previamente cargada para otro propósito, como una KEK, puede restablecerse como una clave de protección de bloqueo de clave TR-31.**

A *No, la carga de una clave en una ranura (registro) debe configurar esta última para su función dada. Si se cambia la función de la ranura, o si se carga una nueva clave de texto simple en la ranura sin autenticación utilizando un control dual, todas las demás claves del dispositivo (o al menos todas las claves que estaban protegidas anteriormente bajo la clave que estaba previamente en la ranura) deben borrarse. Este mecanismo ayuda a garantizar que no pueda controlarse un dispositivo de forma maliciosa.*

P 11 **Mayo 2018 (actualización): se requiere compatibilidad con TR-31 o equivalente como una opción para cualquier dispositivo que permita la carga de claves simétricas que están cifradas por otra clave simétrica como una opción de configuración. Para implementar el TR-31 o equivalente para los dispositivos que actualmente están implementando una metodología simétrica no TR-31, ¿qué características debe tener el dispositivo para admitir esta migración?**

A *El dispositivo debe aplicar lo siguiente cuando corresponda:*

- *La conversión de una metodología menos segura (no TR-31 o no equivalente a TR-31) a una metodología más segura (TR-31 o equivalente) debe ser irreversible.*
- *Cuando se ingresa la clave KBPK de texto plano (o equivalente) a través del teclado, debe realizarse como dos o más componentes mediante al menos dos contraseñas o códigos de autenticación. Estos deben ingresarse a través del teclado o transmitirse cifrados en el dispositivo.*

  Estas contraseñas o códigos de autenticación deben ser únicos por dispositivo (y por custodio), salvo por casualidad o, si están predeterminados por el proveedor, deben estar vencidos y exigir que se cambien en el uso inicial. El adquirente puede cambiar opcionalmente las contraseñas o códigos de autenticación que son únicos por dispositivo (aunque no es necesario) y deben tener al menos siete caracteres.

  La entrada de componentes clave sin por lo menos dos contraseñas o códigos de autenticación independientes tiene como resultado la puesta a ceros de las claves

secretas preexistentes del adquirente, es decir, la invocación de la función o comando de carga de la clave causa la puesta a ceros antes de la carga real de la nueva clave. Para los dispositivos que admiten jerarquías clave de varios adquirente (p. ej., dispositivos de varios adquirentes), solo debe estar en ceros la jerarquía (p. ej., TMK específico y claves de trabajo) asociada con la clave que está cargándose. En todos los casos, los valores de autenticación (contraseñas, códigos de autenticación o similares) para cada usuario en un dispositivo determinado deben ser diferentes para cada usuario.

- *La carga de una KBPK de texto plano (o equivalente) con un cargador de claves debe realizarse con un control dual y exigir dos o más contraseñas o códigos de autenticación antes de la inyección de la clave. Estos se ingresan directamente a través del teclado del dispositivo correspondiente o se transmiten cifrados al dispositivo y deben tener una longitud mínima de siete caracteres. Estas contraseñas o códigos de autenticación deben ser únicos por dispositivo (y por custodio), salvo por casualidad o, si están predeterminados por el proveedor, deben estar vencidos y exigir que se cambien en el uso inicial. Las claves de texto plano o sus componentes nunca se permiten a través de una conexión de red.*

  La inyección de claves secretas de texto plano o sus componentes, en los que el dispositivo receptor en sí mismo no requiere por lo menos dos contraseñas o códigos de autenticación para la inyección, tiene como resultado la puesta en ceros de las claves secretas preexistentes del adquirente. Para los dispositivos que admiten jerarquías clave de varios adquirente (p. ej., dispositivos de varios adquirentes), solo debe estar en ceros la jerarquía (p. ej., TMK específico y claves de trabajo) asociada con la clave que está cargándose. En todos los casos, los valores de autenticación (contraseñas, códigos de autenticación o similares) para cada usuario en un dispositivo determinado deben ser diferentes para cada usuario.

- *No está permitido cargar la KBPK en el dispositivo cifrado por una clave simétrica que no sea TR-31 o no sea equivalente a TR-31. Sin embargo, la KBPK puede cargarse utilizando técnicas asimétricas.*

P 12 **La Guía para el Requisito DTR B9 establece: "Un dispositivo puede incluir más de un esquema de intercambio y almacenamiento de claves que cumpla con los requisitos. Esto no implica que el dispositivo deba aplicar la metodología TR-31 o un esquema equivalente, pero debe ser capaz de implementar tal esquema como una opción de configuración". Si el uso de la metodología TR-31 como mecanismo de intercambio de claves es opcional, ¿debe haber un cambio de configuración de dispositivo explícito para activar o desactivar la metodología TR-31 como el esquema de intercambio de claves "activo"?**

A *Sí, se requiere un cambio de configuración explícito. El cambio se considera un servicio confidencial y debe cumplir con las disposiciones del Requisito B5 de protección de los servicios confidenciales.*

P 13 **Agosto de 2011: cuando un dispositivo se convierte en TR-31 o implementa TR-31 de otra manera, debe ser unidireccional. En un dispositivo que admite múltiples jerarquías de clave independientes, como una diseñado para admitir múltiples adquirentes, ¿la implementación se aplica a todas las jerarquías de clave del dispositivo?**

A *No, un dispositivo compatible con múltiples jerarquías independientes puede implementar la metodología TR-31 (o equivalente) jerarquía por jerarquía.*

P 14 ¿Existen restricciones sobre cómo se carga la clave maestra de terminal en el dispositivo?

A *La clave maestra inicial de la terminal (TMK) debe cargarse en el dispositivo mediante técnicas de clave asimétrica o técnicas manuales; por ejemplo, el teclado del dispositivo, las tarjetas IC, el dispositivo de carga de la clave, etc. La carga posterior de la clave maestra del terminal puede utilizar técnicas asimétricas, técnicas manuales o la TMK actual para cifrar la TMK de reemplazo para la descarga. Las claves no pueden cargarse de nuevo con ninguna metodología en caso de que el dispositivo se haya puesto en riesgo, el cual debe retirarse de su uso.*

P 15 Algunos dispositivos permiten utilizar una función de descifrado de datos que, si no se controla, puede permitir la salida de información confidencial, como claves o PIN, en texto simple. ¿Cómo debe protegerse un dispositivo contra la salida de datos confidenciales?

A *Debe manejarse mediante al menos una de las cinco técnicas:*

- *La información sobre el uso de la clave de cualquier clave descargada debe estar vinculada criptográficamente al valor de la clave mediante métodos aceptados, y el dispositivo debe hacer cumplir que la clave se utilice únicamente para el uso previsto.*
- *La incorporación de un nuevo tipo de clave (ranura) posterior a la configuración inicial del dispositivo provoca la puesta a ceros de todas las demás claves secretas. Los dispositivos que admitan técnicas de distribución remota de claves mediante técnicas asimétricas solo admiten el uso de dichas técnicas para la carga de TMK. No se admitirá el uso de técnicas de distribución de claves a distancia para las claves de trabajo (por ejemplo, PIN, datos, MAC, etc.) a menos que la información de uso de la clave esté vinculada criptográficamente a cada clave individual.*
- *El dispositivo no debe aceptar los tipos de claves de datos descargados, a menos que se cifren con una clave maestra de terminal diferente de las claves confidenciales, como los tipos de claves PEK o MAC.*
- *El dispositivo no proporciona soporte para descifrar datos o una función similar.*
- *El dispositivo debe verificar que las claves para diferentes propósitos no tengan nunca el mismo valor; este requisito debe mantenerse hasta que el dispositivo se haya desmantelado (o hasta que se modifiquen las TMK correspondientes).*

P 16 Mayo de 2018 (actualización): ¿pueden utilizarse claves secretas o sus componentes para otros fines, como contraseñas o códigos de autenticación, a fin de permitir el uso de servicios confidenciales?

A *No. El uso de claves secretas o sus componentes para otros fines incumple el requisito de que las claves se utilicen para su único propósito previsto, por ejemplo, codificación de claves o codificación de PIN, etc.*

P 17 **Septiembre de 2016 (actualización): los requisitos de seguridad del PIN de PCI estipulan que cualquier dispositivo criptográfico utilizado para la adquisición de datos de PIN que se retire del servicio debe tener todas las claves almacenadas dentro del dispositivo destruido que se haya utilizado (o que posiblemente pudiera usarse) para cualquier fin criptográfico. Si es necesario para cumplir con lo anterior, el dispositivo debe destruirse físicamente para que no pueda volver a ponerse en servicio o permitir la divulgación de datos o claves secretos. ¿Esto se aplica solo a las claves simétricas?**

A *No, esto se aplica a cualquier clave secreta o privada utilizada por el dispositivo para el cifrado del PIN, validación del firmware, control de selección dinámica de pantalla o la protección de cualquiera de esas mismas claves durante la carga en el dispositivo o el almacenamiento dentro del dispositivo, incluyendo las claves privadas utilizadas en relación con la distribución de claves remotas mediante técnicas asimétricas. Este requisito se aplica tanto a las claves originadas o controladas por el proveedor como por el adquirente. Esto no incluye las claves públicas presentes o utilizadas por el dispositivo.*

El proveedor debe proporcionar instrucciones de desmantelamiento y mecanismos asociados para hacer que todas esas claves no recuperables para un atacante sean verificables para el laboratorio de evaluación. Estas técnicas incluyen, entre otras:

- *Comandos de menú específicos para poner a ceros las claves almacenadas;*
- *Inducción de un evento de manipulación para poner a ceros esas claves;*
- *El cifrado por una clave de igual o mayor solidez que está en sí misma en ceros, es decir, solo pueden recuperarse criptogramas de las claves protegidas.*

P 18 **Mayo de 2018: la metodología ANSI TR-34 describe dos protocolos para implementar la distribución de claves simétricas con técnicas asimétricas. Las dos técnicas se describen como el método de dos pasos y el método de un paso, y deben utilizarse de la siguiente manera:**

- **El método de dos pasos es apropiado para que el POI y el KDH puedan comunicarse en tiempo real. Utiliza nonces aleatorios para evitar ataques de reproducción.**
- **El método de un paso es adecuado para entornos en los que el POI y el KDH no podrán comunicarse en tiempo real, es decir, el POI no puede iniciar la secuencia de mensajes de protocolo criptográfico. En estos entornos, el KDH generará el mensaje criptográfico que puede transportarse al POI a través de canales no confiables en tiempo real. Incluye el uso de marcas de tiempo en lugar de nonces aleatorios para evitar ataques de reproducción.**

La entrada de claves maliciosas de un dispositivo POI por un segundo KDH bajo la misma PKI es posible cuando el POI ya ha intercambiado credenciales con un primer KDH. Para evitar este ataque, se requiere la vinculación (o un método equivalente como se indica en la guía DTR B9) para todos los dispositivos POI, y es un requisito previo para los protocolos de intercambio de claves de dos pasos y uno de uno de los pasos.

¿Se requieren dispositivos POI para admitir ambos métodos?

A *No, un dispositivo puede admitir solo uno. Independientemente de que el dispositivo sea compatible solo con uno o ambos, el proveedor debe describir en la política de seguridad del dispositivo, que se publica en el sitio web de PCI, los entornos y circunstancias bajo los cuales es apropiado implementar uno o más métodos compatibles.*

P 19 Septiembre de 2020: el Requisito 18-3 de seguridad del PIN exige la implementación de bloques de claves. Los métodos interoperables incluyen los definidos en las normas ASC X9 TR-31 e ISO 20038. El requisito también permite cualquier método equivalente en el que se incluya la vinculación criptográfica de la información sobre el uso de la clave con el valor de la clave con métodos aceptados. ¿Cómo se determinan los métodos equivalentes?

A *Los métodos equivalentes deben estar sujetos a una revisión independiente por parte de un experto, y dicha revisión está disponible públicamente para la revisión por parte de los compañeros:*

- *La revisión del experto independiente debe incluir pruebas de que en el método equivalente la clave cifrada y sus atributos en el bloque de claves tienen una protección de integridad tal, que es inviable desde el punto de vista informático que la clave se utilice si esta o sus atributos se han modificado. La modificación incluye, entre otros aspectos:*
  - *Cambiar o reemplazar cualquier bit(s) en los atributos o la clave cifrada.*
  - *Intercambiarlos bits del bloqueo de claves protegidas con bits de otra parte del bloqueo.*
- *El experto independiente debe estar calificado mediante preparación académica, capacitación y experiencia en criptografía para realizar evaluaciones técnicas objetivas que sean independientes de cualquier vínculo con proveedores e intereses especiales. A continuación, se define con más detalle el concepto de experto independiente.*
- *El laboratorio de PTS validará que cualquier proveedor de dispositivos que implemente esta metodología lo haya hecho siguiendo todas las pautas de dicha evaluación y revisión por pares, incluyendo las recomendaciones para la administración de claves asociadas.*

Un experto independiente posee las siguientes calificaciones:

- *Tiene una o varias credenciales profesionales aplicables al campo; por ejemplo, un doctorado en una disciplina pertinente o una certificación en criptografía otorgada por una autoridad gubernamental (NSA, CES o GCHQ).*
- *Cuenta con 10 o más años de experiencia en el tema pertinente.*
- *Se apega a un código ético de conducta, y se sometería a un proceso de ética y cumplimiento si fuera necesario.*
  - *Ha publicado al menos dos artículos relacionados con el tema en publicaciones revisadas por colegas.*
  - *Es reconocido por sus colegas en el campo (p. ej., es miembro o miembros distinguido de organizaciones tales como ACM, BCS, IEEE, IET, o IACR).*

La independencia requiere que la entidad no esté sujeta a controles, restricciones, modificaciones o limitaciones de una determinada fuente externa. Concretamente, la independencia requiere que una persona física o moral solicite su contratación como criptólogo o un experto similar por varias empresas clientes no colabore regularmente con una sola de ellas, no trabaje en forma exclusiva para una empresa y en cada caso reciba una remuneración basada en el tiempo que dedique al trabajo y los gastos en que incurra para realizarlo.

P 20 Septiembre de 2020: los dispositivos deben ser compatibles con la metodología de derivación de claves ANSI TR-31 para las claves TDES; para las claves AES, deben admitir la metodología TR-31 o la metodología ISO 20038. En todo caso, pueden utilizarse métodos equivalentes cuando se sometan a la revisión de un experto independiente y dicha revisión esté a disposición del público tal como se ha descrito. ¿Qué características que se hacen cumplir en TR-31 e ISO 20038 deben considerarse para determinar la equivalencia?

A *La "equivalencia" debe demostrarse en el contexto de las pruebas de seguridad. El método equivalente debe cumplir las funciones de integridad de las claves, como restringir su uso reiterado y garantizar su confidencialidad. Específicamente, un esquema de bloqueo de claves equivalente debe ofrecer como mínimo las siguientes propiedades:*

a) *Debe evitar que la carga de las claves PIN, MAC y/o datos o cualquier clave usada para manejarlas dentro de la jerarquía de claves se utilice para otro propósito. Las claves de IPEK, KEK y derivación deben identificarse de manera única en donde se admitan.*
b) *Debe evitar la determinación de la longitud de la clave para las claves de longitud variables.*
c) *Debe verificarse que la clave pueda utilizarse solo para un algoritmo específico (como TDES o AES, pero no para ambos).*
d) *Debe verificarse que pueda rechazarse un bloqueo de clave modificado antes de utilizarlo, independientemente de la utilidad de la clave después de la modificación. La modificación incluye cambiar cualquier bit de la clave, así como el reordenamiento o manipulación de claves DES individuales dentro de un bloqueo de clave TDES.*
e) *Cuando se admiten diferentes formatos de bloqueos de claves, algunos de los cuales ofrecen las protecciones anteriores y otros no, debe ser humanamente legible desde el bloqueo de claves antes de cargar o utilizar el formato que se implementa; por ejemplo, observando los comandos enviados al dispositivo.*
f) *Debe admitir todos los algoritmos simétricos implementados por los dispositivos que van a utilizar los bloqueos de claves.*
g) *Cuando se admiten algoritmos asimétricos, el tipo de algoritmo, el ensamblador y los formatos de firma deben identificarse en el bloqueo de clave.*
h) *Debe utilizar los modos de operación aprobados por el NIST, con claves separadas utilizadas para la confidencialidad y autenticidad. Las claves utilizadas no deben estar relacionadas de manera reversible.*

El bloqueo de clave equivalente puede admitir opcionalmente otras características, como:

i. *Un número de versión de la clave que evita el uso de claves antiguas o vencidas;*
ii. *Apoyo a la "dirección" de la clave (claves unidireccionales) para que una clave MAC pueda identificarse como "solo de verificación" o una clave de datos como "solo de cifrado";*
iii. *Soporte para propósitos de claves que no sean PIN, MAC y datos;*
iv. *Compatibilidad con TDES y AES (cuando los dispositivos que implementan los bloques clave solo admiten uno de estos algoritmos, solo transicionales, los nuevos dispositivos deben ser compatibles con AES);*
v. *Implementar controles de confidencialidad sobre cualesquier metadatos clave que no sean la longitud de la clave.*
vi. *Compatibilidad con algoritmos asimétricos.*

P 21 **Septiembre de 2020: los dispositivos POI son necesarios para admitir bloqueos de claves mediante la metodología de derivación de claves ASC X9 TR-31 para las claves TDES, y para las claves AES deben ser compatibles con la metodología TR-31 o con la metodología ISO . Las metodologías TR-31 e ISO 20038 son para empaquetar claves (los bloques de claves) para su transporte o almacenamiento, pero utilizan mecanismos simétricos para ello; para el transporte de las claves, requieren una clave simétrica de intercambio que se comparte previamente para su uso como clave de protección del bloqueo de llaves. En los casos en que no se haya establecido previamente una clave simétrica con un dispositivo POI para la distribución de claves a distancia y vayan a utilizarse métodos asimétricos, ¿se debe admitir una metodología de bloqueos de claves?**

A *Sí. Debe utilizarse un método como ASC X9 TR 34: Método interoperable para la distribución de claves simétricas utilizando técnicas asimétricas: Parte 1; uso de transporte de claves unilaterales de criptografía de clave pública basada en factores. Conforme a TR-34, similar a TR-31 e ISO 20038, el bloqueo de clave consta de tres partes:*

- *El encabezado de bloqueo de clave (KBH) que contiene información de atributos sobre la clave y el bloqueo de clave*
- *Los datos confidenciales que se están intercambiando o almacenando*
- *El método de unión de bloqueos de claves*

Sin embargo, la metodología TR-34 utiliza métodos asimétricos para el método de vinculación de bloqueos de claves, en lugar de los métodos simétricos utilizados en TR-31 o ISO 20038 que requieren que una clave simétrica se haya intercambiado entre el dispositivo POI y el KDH.

Requisito de POI B10

P 1 **Junio de 2016 (actualización): el Requisito B10 establece que cualquier método utilizado para producir texto cifrado que se base en modos de operación "no estándar" (por ejemplo, el modo de cifrado basado en la conservación del formato [FFF]) deberá estar aprobado al menos por una organización independiente de evaluación de la seguridad (por ejemplo, un órgano de normalización) y someterse a una revisión de expertos independientes. ¿Cómo se cumple este requisito si el método no está incluido en una norma publicada?**

A *Todos los datos de la cuenta se cifrarán utilizando solo algoritmos de cifrado aprobados por ANSI X9 o ISO (por ejemplo, AES, TDES). Además, el modo de operación que se utiliza será cualquiera de los siguientes:*

1. *Uno descrito en la norma ISO/IEC 10116: 2006 (o equivalente) y que sigue las directrices de ensamblado seguro;*

O

2. *Existe en un proyecto de norma de un organismo de normalización aplicable a la industria de pagos financieros, es decir, ANSI, ISO o NIST;*

Y

3. *Está sujeto a una revisión independiente por parte de un experto y dicha revisión está disponible públicamente y la verifica el laboratorio de evaluación PCI PTS.*

La revisión del experto independiente debe incluir pruebas de que este FPE protege en cuanto a la "recuperación de mensajes", según se define en Bellare, M., Ristenpart, T., Rogaway, P., y Stegers, T. (agosto de 2009). Format-preserving encryption. En Selected Areas in Cryptography (págs. 295-312). Springer Berlin Heidelberg (https://eprint.iacr.org/2009/251.pdf).

El experto independiente debe estar calificado mediante preparación académica, capacitación y experiencia en criptografía para realizar evaluaciones técnicas objetivas que sean independientes de cualquier vínculo con proveedores e intereses especiales. El experto independiente también se define en el glosario.

El laboratorio de PTS validará que el proveedor del dispositivo ya implementó la solución FPE siguiendo todas las pautas de dicha evaluación y revisión por pares, incluyendo cualquier recomendación para la administración de claves asociadas.

Requisito de POI B12

P 2 ¿Un dispositivo puede utilizar una clave de cifrado para cifrar o descifrar información de la etiqueta de clave junto con una clave?

A *Sí, la información de la etiqueta clave asociada, como el algoritmo, la caducidad de la clave, el uso o el MAC de la clave, puede cifrarse o descifrarse junto con la clave mediante una clave de cifrado. La clave y su etiqueta están vinculadas mediante un modo de encadenamiento de cifrado como se define en la ISO 10116.*

Requisito de POI B15

P 1 ¿Cuál es la definición de "unidad criptográfica"?

A *La unidad criptográfica es el microprocesador que cifra el bloqueo de PIN. Este procesador está sujeto a requisitos de PCI para dispositivos y, por lo tanto, se considera seguro cuando se encuentra dentro de un dispositivo compatible. Esto significa que puede utilizarse un microcontrolador de propósito general siempre que esté dentro de un dispositivo que cumpla con los requisitos de PCI para dispositivos.*

P 2 ¿Es aceptable utilizar un mensaje controlado por LED exclusivamente por el procesador seguro criptográfico como mensaje para la entrada del PIN?

A *No. Los titulares de tarjetas esperan que el mensaje del PIN provenga de la misma pantalla que otros mensajes. Si no es así, hay una mayor posibilidad de que los titulares de las tarjetas se direccionen incorrectamente.*

P 3 ¿Calificaría la visualización de los dígitos del PIN en texto plano por el dispositivo como prueba de manipulación?

A *No. El es posible que el titular de la tarjeta no esté familiarizado con el comportamiento típico de un dispositivo determinado y no reconozca que el dispositivo está infringiendo el Requisito B3.*

P 4 Si una terminal incluye una pantalla bajo su control y un teclado con su propia pantalla, ¿la unidad criptográfica del dispositivo debe controlar ambas pantallas?

A *Sí. Si un solo dispositivo tiene dos pantallas que podrían solicitar datos al titular de la tarjeta, ambas pantallas se regirían por el Requisito B15. Esto significa que la terminal y el teclado son un único dispositivo que debe cumplir con los requisitos de PCI.*

P 5 **Las claves criptográficas utilizadas para actualizar los avisos en pantalla deben administrarse bajo los principios de control dual y conocimiento dividido, y las claves secretas o privadas que se utilicen no deben aparecer en texto simple fuera de un dispositivo criptográfico seguro. ¿Los datos de autenticación que se utilizan para habilitar el uso de una clave de firma o aplicando el MAC viajan a través de un entorno sin protección, es decir, la RAM sin protección de un equipo?**

A *Los datos de autenticación pueden existir en el exterior de un dispositivo seguro criptográfico. Sin embargo, el proveedor debe proporcionar a los clientes de laboratorio instrucciones para utilizar una sala segura, PC dedicada, implementación de técnicas de control dual, procedimientos de inspección de equipos, etc.*

P 6 **¿Qué requisitos de registro debe cumplir un SCD conforme al Requisito B15?**

A *Los registros deben proporcionar suficiente material probatorio para demostrar al laboratorio que existen las técnicas y mecanismos de control especificados por el vendedor.*

P 7 **Mayo de 2018 (actualización): ¿pueden considerarse los tokens de autenticación USB o las tarjetas inteligentes como el SCD requerido para hacer cumplir el control dual conforme al Requisito B15?**

A *El uso de tokens duales por sí solos no cumpliría con los requisitos. Los tokens deberían aplicar el uso de contraseñas o códigos de autenticación e incluir seguridad para proteger su contenido.*

P 8 **Mayo de 2011: si un dispositivo cumple con el Requisito B15, ¿cuáles son los requisitos para controlar las actualizaciones de estos avisos?**

A *El Requisito B15 se evalúa cuando un dispositivo utiliza actualizaciones de firmware para controlar el cambio de los mensajes en la pantalla. Por lo tanto, la actualización de mensajes para los dispositivos que cumplen con el Requisito B15 requiere la creación de una nueva versión de firmware y un cambio resultante en el número de versión de firmware del PED.*

No es aceptable que los mensajes controlados por el proveedor se actualicen por separado del firmware, sin la generación de una nueva versión del mismo. Es aceptable que las actualizaciones rápidas usen una clave criptográfica independiente a la que se utilice para otras actualizaciones de firmware, pero cualquier método de actualización independiente debe estar calificado por el laboratorio como compatible con los Requisitos E2 y B2. En todo momento, las claves criptográficas utilizadas para actualizar los mensajes y el firmware deben ser diferentes de las utilizadas para actualizar el código de no firmware, como las aplicaciones.

P 9 **2011 de mayo: si un dispositivo cumple con el Requisito B15, ¿significa que tengo que volver a enviar el dispositivo para la evaluación de laboratorio cada vez que cambio los mensajes?**

A *Si hay comodines adecuados en la lista de versiones de firmware para adaptarse a nuevas versiones rápidas que se revisaron y confirmaron previamente según corresponda por parte de un laboratorio de PCI, la revisión de cada cambio por parte de dicho laboratorio no es necesaria.*

P 10 **Mayo de 2011: el Requisito B15 no especifica ninguna posibilidad mínima de ataque. ¿Qué requisitos se aplican a la seguridad física de un dispositivo que permite que terceros actualicen los mensajes en pantalla utilizando controles basados en criptografía?**

A *Todos los mensajes que pueden utilizarse para solicitar la entrada de datos de texto plano al titular de la tarjeta deben protegerse contra una posibilidad de ataque de al menos 18 puntos PCI con un mínimo de 9 puntos de explotación. Esto incluye mensajes que pueden ser actualizados por terceros mediante controles basados en criptografía.*

P 11 **Marzo de 2015: los ensambladores de PIN diseñados para su uso con los cajeros automáticos suelen admitir tanto un estado seguro (codifica los datos introducidos) como no seguro. ¿La transición entre los estados requiere una autenticación?**

A *Sí, para la autenticación deben utilizarse mecanismos criptográficos acordes con el apéndice D de los requisitos de prueba derivados de los puntos de interés. Específicamente:*

- *Se requiere un canal seguro entre la interfaz del ensamblador del PIN y el controlador (ATM) para administrar los cambios entre los modos PIN y de entrada de datos de texto plano.*
- *Para las pantallas táctiles, la administración de los "botones" del teclado se realiza de forma segura para evitar la determinación del PIN del cliente mediante la explotación de posibles diferencias en el teclado numérico mostrado y la organización de los botones numéricos en la interfaz táctil.*

Esto no implica que el dispositivo debe forzar la implementación, sino que debe proporcionar soporte para dicha implementación.

Requisito de POI B17

P 1 **Agosto de 2011: el sistema operativo del dispositivo debe contener solo los componentes necesarios y debe configurarse de forma segura y ejecutarse con menos privilegios. ¿Qué se considera un "sistema operativo" con fines de PCI?**

A *En el ámbito del PCI-PTS, cualquier software subyacente que proporcione servicios para el código que se ejecuta en el dispositivo se considera parte del sistema operativo. Entre los ejemplos de esos servicios, figuran la inicialización y el arranque del sistema, las capas de abstracción de hardware, la gestión de la memoria, la multitarea, las primitivas de sincronización, los sistemas de archivos, los controladores de dispositivos y las pilas de red. Los servicios que proporcionan seguridad o que pueden afectar a la seguridad se consideran, además, firmware.*
Los sistemas operativos pueden ir desde las bibliotecas de la capa de abstracción de hardware y los micronúcleos incrustados hasta los complejos sistemas operativos multiusuario.

Requisito de POI B18

P 1 ¿Cuáles son los métodos aceptables para cumplir con este requisito?

A *Por lo general, el uso de técnicas de administración de claves aceptadas cumplirá con este requisito:*

- *Cuando se utiliza la técnica de administración de clave maestra o de sesión, este requisito se cumple porque el éxito en la sustitución de la clave requiere que el atacante conozca la clave maestra contenida en el dispositivo.*
- *Este requisito se cumple cuando se utiliza la técnica de administración de clave DUKPT, porque las claves de PIN se derivan de la información secreta contenida en el dispositivo.*

Sin embargo, cuando el dispositivo está destinado a admitir varios adquirentes y un usuario selecciona el adquirente (es decir, el comerciante presiona un botón), el dispositivo debe verificar que se haya elegido el adquirente correcto.

P 2 ¿Es aceptable que un dispositivo que admita múltiples jerarquías de clave cumpla con el Requisito B18 garantizando que las aplicaciones específicas solo puedan acceder a las claves asociadas a ellas?

A *Sí. Es aceptable siempre y cuando cada aplicación solo pueda acceder a las claves de una única jerarquía de claves.*

P 3 ¿Cuáles son los medios aceptables para la selección de claves criptográficas externas?

A *Las claves pueden seleccionarse con el teclado del dispositivo o mediante comandos enviados desde otro dispositivo, como una caja registradora electrónica. Cualquier comando enviado desde otro dispositivo debe autenticarse criptográficamente para que haya protección contra ataques tipo intermediario y de reproducción.*

P 4 Si una clave seleccionada externamente no es la clave de cifrado utilizada para cifrar directamente el bloqueo de PIN, ¿se requiere que esta selección se autentique?

A *Si la selección externa está asociada al cifrado de PIN, la autenticación sería aplicable. Por ejemplo, si selecciona externamente la clave maestra con la que se descifrará una clave de sesión para usarse en el cifrado de bloqueo de PIN, deberá autenticarse.*

P 5 ¿Es aceptable que las claves de PIN se seleccionen externamente de forma indirecta seleccionando al adquirente si tal selección se realiza con un comando autenticado criptográficamente? Se asume que hay varias jerarquías de claves relacionadas con el cifrado de PIN bajo cada adquirente.

A *Sí, siempre y cuando haya un mecanismo que asegure que las claves bajo cada adquirente se asocien exclusivamente con este.*

P 6 **Mayo (actualización) de 2018: la selección de claves externas incluye la selección realizada por un host local o remoto. ¿En qué circunstancias no se requiere que un dispositivo compatible con varias jerarquías de claves exija autenticación a cada comando de selección de claves externas?**

A *Si una aplicación puede seleccionar claves de varias jerarquías de claves, el dispositivo debe exigir la autenticación de los comandos utilizados para la selección de claves externas. Si el dispositivo solo permite a una aplicación para seleccionar claves de una única jerarquía, entonces no se requiere la autenticación del comando.*

Por otra parte, la autenticación no es necesaria en ninguna de las dos circunstancias siguientes:

- *Solo el proveedor establece directamente las jerarquías de claves para el cifrado de PIN en sus instalaciones seguras o en unas instalaciones autorizadas operadas por un tercero que de manera regular realice la carga de claves en nombre del proveedor y esté registrado para hacerlo según las normas aplicables de marca de pago, y después de abandonar las instalaciones sea física y/o lógicamente imposible cargar jerarquías de claves adicionales sin volver a las instalaciones.*
- *Las jerarquías de claves solo pueden establecerse de conformidad con el Requisito B7. Las nuevas jerarquías de claves deben autenticarse mediante un control dual (contraseñas o códigos de autenticación), ya sea a través del cargador de claves o directamente a través del EPP o POS PED. Las jerarquías de claves actuales pueden sustituirse sin utilizar la autenticación si la carga da lugar a la puesta a cero de las claves secretas preexistentes: es decir, la invocación de la función o comando de carga de la clave causa la puesta a cero antes de la carga real de la nueva clave. Además, las jerarquías de claves pueden sustituirse o bien, pueden establecerse nuevas jerarquías de claves mediante la distribución de claves a distancia utilizando técnicas asimétricas que cumplan con los requisitos de seguridad de PIN de PCI, anexo A.*

P 7 **¿Cuándo no se aplica el Requisito B18 a los dispositivos de aviso de pantalla controlados por el adquirente?**

A *El Requisito B18 no se aplica a los dispositivos B de mensajes en pantalla controlados por el adquirente que no incluyan comandos para la selección de claves externas, o que no puedan contener varias claves relacionadas con el cifrado de PIN.*

Requisito de POI B20

P 1 **Junio de 2015: ¿se ve afectada la aprobación del dispositivo si el proveedor cambia la política de seguridad evaluada por el laboratorio?**

A *A partir de la V4, el contenido de la política de seguridad forma parte de la evaluación de un dispositivo por parte del laboratorio, y es una entrada integral en la que se basa la aprobación de un dispositivo. Los implementadores se apoyan en la política de seguridad para garantizar que no incumplan las condiciones para la aprobación de un dispositivo. Cualquier cambio en la política de seguridad que afecte los requisitos de seguridad del dispositivo debe evaluarse para que el dispositivo mantenga su aprobación. Además, cualquier cambio en la funcionalidad ofrecida por el dispositivo que afecte la información que debe contener la política de seguridad tiene que reflejarse en una actualización en el documento de la política de seguridad que figura en la lista.*

Según la naturaleza de los cambios, esto puede reflejarse en actualizaciones (por ejemplo, en apéndices) a una política de seguridad o como políticas de seguridad adicionales publicadas en el sitio web. En todos los casos, todas las versiones aprobadas de los productos deben abordarse en las políticas de seguridad publicadas en el sitio web de la PCI.

P 2 **Octubre (actualización) de 2018: los requisitos del laboratorio de PCI PTS prohíben que un laboratorio de PTS cree documentación de cualquier proveedor. ¿Existen situaciones en las que un laboratorio de PTS puede ayudar a un proveedor a crear documentación?**

A *En algunos casos, un laboratorio de PTS puede revisar la Política de seguridad para realizar correcciones gramaticales, de formato o de ortografía de un dispositivo en evaluación. Esto puede hacerse para ayudar al proveedor a crear un documento suficiente para presentarse ante PCI. En este caso, el laboratorio PTS proporcionará lo siguiente como parte de la presentación del informe de evaluación:*

- *Una versión modificada/revisada de la Política de seguridad editada que muestra el texto original creado por el proveedor y el texto actualizado.*
- *Una copia limpia de la Política de Seguridad editada para su publicación.*

Requisito de POI B21

P 1 **ISO 9564 estipula que, si el PIN va a enviarse a la tarjeta IC de forma cifrada, el dispositivo deberá cifrar el PIN mediante la clave de cifrado autenticado de la tarjeta IC y enviar el PIN cifrado a la tarjeta IC. ¿Existen restricciones sobre el lugar donde debe realizarse la autenticación?**

A *El dispositivo debe proteger la integridad de todas las claves públicas (ICC, emisor aplicable y marca de pago) mediante las técnicas definidas en la norma ISO 11568. En todos los casos, la autenticación debe realizarse en un componente seguro del dispositivo, como el ensamblador de PIN o ICCR. Esto incluye la autenticación de la(s) clave(s) pública(s) de ICC, así como la clave pública del emisor asociada en la cadena de certificados hasta la clave de marca de pago aplicable.*

Requisito de POI B23

P 1 **Junio de 2012: la guía establece que se define el modo de cifrado cuando el cifrado de la funcionalidad de datos de la cuenta del dispositivo está habilitado y en operación. ¿Un dispositivo puede generar la salida de todos o algunos datos de la cuenta sin cifrado cuando se encuentra en modo de cifrado?**

A *Sí, incluso los dispositivos que solo admiten el modo de cifrado. Por ejemplo, un dispositivo puede implementar listas blancas autenticadas criptográficamente para la salida sin cifrado de datos de cuentas, incluso si esa lista blanca hace que todos los datos de las cuentas salgan sin cifrado. La ausencia de la lista blanca hace que todos los datos de las cuentas estén cifrados.*

Requisito de POI E2

P 1 **Muchos dispositivos están diseñados para que terceros puedan crear y cargar aplicaciones. Los proveedores a menudo respaldan esto cuando proporcionan a terceros las herramientas necesarias para crear y cargar aplicaciones. ¿Cómo puede un proveedor asegurarse de que no es responsable de controlar la aplicación?**

A *Si las aplicaciones no se consideran firmware, no es necesario que el proveedor las controle. El diseño del dispositivo debe evitar que las aplicaciones afecten a las funciones y características regidas por los requisitos. Entre los ejemplos de funciones que no deben verse influidas por aplicaciones "no firmware", figuran la gestión de claves (selección de claves, autenticación de claves, generación de claves, carga de claves, etc.), pruebas automáticas, tiempo entre cifrados de bloques de PIN, acceso a servicios confidenciales, límites a los servicios sensibles, actualización y autenticación de firmware, respuesta a la manipulación, etc.*

La alteración de los mensajes de terceros es un caso especial que puede verse afectado por aplicaciones que no son de firmware siempre y cuando se cumpla con el Requisito POI B15 de PCI.

Las aplicaciones SRED desarrolladas por terceros también son una excepción. Deben cumplir con todos los criterios aplicables en el módulo SRED, incluidas las preguntas frecuentes asociadas.