



Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos para las Aplicaciones de Pago

**Requisitos y procedimientos de evaluación de
seguridad**

Versión 2.0

Octubre de 2010

Modificaciones realizadas a los documentos

<i>Fecha</i>	<i>Versión</i>	<i>Descripción</i>	<i>Páginas</i>
1 de octubre de 2008	1.2	Alinear el contenido con la nueva versión 1.2 de PCI DSS e implementar cambios menores notados desde la versión 1.1 original.	
Julio de 2009	1.2.1	Debajo de “Alcance de las PA-DSS”, alinear el contenido con la Guía del programa PA-DSS, versión 1.2.1, para especificar claramente las aplicaciones a las que se aplican las PA-DSS.	v, vi
		Debajo del Requisito de laboratorio 6, se corrigió la ortografía de “OWASP”.	30
		En la Declaración de validación, Parte 2a, actualizar Funcionalidad de la aplicación de pago para que concuerde con los tipos de aplicación especificados en la Guía del programa PA-DSS, y aclarar los procedimientos de revalidación anual en la Parte 3b.	32, 33
Octubre de 2010	2.0	Actualizar e implementar cambios menores de la versión 1.2.1 y alinear con las nuevas PCI DSS versión 2.0. Para obtener los detalles, consulte “PA-DSS—Resumen de cambios de las PA-DSS versión 1.2.1 a 2.0.”	

Índice

Modificaciones realizadas a los documentos	2
Introducción	4
Finalidad de este documento	4
Relación entre PCI DSS y PA-DSS.....	4
Alcance de las PA-DSS.....	5
Aplicabilidad de las PA-DSS a las aplicaciones de pago en terminales de hardware.....	7
Funciones y responsabilidades	8
Guía de implementación de las PA-DSS	11
Requisitos del Asesor de Seguridad Certificado para las Aplicaciones de Pago (PA-QSA)	11
Laboratorio de pruebas	12
Información sobre la aplicabilidad de las PCI DSS	13
Instrucciones y contenido para el informe de validación.....	15
Pasos para completar las PA-DSS	17
Guía del programa PA-DSS.....	17
Requisitos y procedimientos de evaluación de seguridad de las PA-DSS	18
1. No retenga toda la banda magnética, el código o valor de validación de la tarjeta (CAV2, CID, CVC2, CVV2), ni los datos de bloqueo del PIN. 18	
2. Proteja los datos del titular de la tarjeta que fueron almacenados	23
3. Proporcione funciones de autenticación segura	29
4. Registre la actividad de la aplicación de pago.....	34
5. Desarrolle aplicaciones de pago seguras	37
6. Proteja las transmisiones inalámbricas.....	41
7. Pruebe las aplicaciones de pago para tratar las vulnerabilidades	43
8. Facilite la implementación de una red segura	44
9. Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet	44
10. Facilite un acceso remoto seguro a la aplicación de pago.	45
11. Cifre el tráfico sensitivo de las redes públicas	49
12. Cifre el acceso administrativo que no sea de consola.....	50
13. Mantenga la documentación instructiva y los programas de capacitación para clientes, revendedores e integradores.....	50
Anexo A: Resumen de contenidos para la <i>Guía de implementación de las PA-DSS</i>	52
Anexo B: Confirmación de la configuración del laboratorio de pruebas específica de la evaluación de las PA-DSS	59

Introducción

Finalidad de este documento

Los Asesores de Seguridad Certificados para las Aplicaciones de Pago (PA-QSA), quienes realizan las revisiones de la aplicación de pago, utilizarán este documento para que los proveedores de software puedan validar que una aplicación de pago cumple con las Normas de Seguridad para las Aplicaciones de Pago (PA-DSS) de PCI. Este documento también tiene la finalidad de ser utilizado por los PA-QSA como plantilla para crear el Informe de validación.

Otros recursos, como las Declaraciones de validación, las Preguntas frecuentes (FAQ) y el *Glosario de términos, abreviaturas y acrónimos de PCI DSS y PA-DSS* están disponibles en el sitio web del PCI Security Standards Council (PCI SSC) en www.pcisecuritystandards.org.

Relación entre PCI DSS y PA-DSS

El uso de una aplicación que cumpla con las PA-DSS por sí solo no implica que una entidad cumpla con las PCI DSS, dado que esa aplicación se debe implementar en un entorno que cumpla con las PCI DSS y de acuerdo con la Guía de implementación de las PA-DSS proporcionada por el proveedor de la aplicación de pago (según el Requisito de PA-DSS 13.1).

Los requisitos de las Normas de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS) se derivan de los Requisitos de las *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)* y de los *Procedimiento de Evaluación de Seguridad*. Este documento, que se puede encontrar en www.pcisecuritystandards.org, detalla lo que se debe hacer para cumplir con las PCI DSS (y, por consiguiente, lo que debe admitir una aplicación de pago para facilitar el cumplimiento de las PCI DSS por parte de un cliente).

Es posible que el cumplimiento tradicional de las Normas de Seguridad de Datos de PCI no se aplique directamente a proveedores de aplicaciones de pago, dado que la mayoría de ellos no almacena, procesa ni transmite datos de titulares de tarjetas. Sin embargo, dado que los clientes utilizan estas aplicaciones de pago para almacenar, procesar y transmitir datos de titulares de tarjetas, y dichos clientes deben cumplir con las Normas de Seguridad de Datos de PCI, las aplicaciones de pago deben facilitar, y no entorpecer, el cumplimiento de las Normas de Seguridad de Datos de PCI por parte de los clientes. Las siguientes son algunas de las maneras en que las aplicaciones de pago pueden impedir el cumplimiento.

1. Almacenamiento de datos de banda magnética o datos equivalentes que están el chip en la red del cliente después de la autorización;
2. Aplicaciones que les exigen a los clientes desactivar otras funciones requeridas por las Normas de Seguridad de Datos de PCI, como un software de antivirus o los sistemas de seguridad de tipo "firewalls", para que funcione adecuadamente la aplicación de pago; y
3. El uso por parte de los proveedores de métodos inseguros para establecer conexión con la aplicación a fin de proporcionar apoyo al cliente.

Cuando se implementen en un entorno que cumpla con las PCI DSS, las aplicaciones de pago seguro minimizarán tanto la posibilidad de fallos de seguridad que comprometan todos los datos de la banda magnética, los códigos y valores de validación de la tarjeta (CAV2, CID, CVC2, CVV2), los PIN y los bloqueos de PIN, como el fraude perjudicial derivado de tales fallos de seguridad.

Alcance de las PA-DSS

Las PA-DSS se aplican a proveedores de software y demás que desarrollan aplicaciones de pago que almacenan, procesan o transmiten datos de titulares de tarjetas como parte de la autorización o de la liquidación, siempre que dichas aplicaciones se vendan, distribuyan u otorguen bajo licencia a terceros.

Se puede utilizar la siguiente guía para determinar si las PA-DSS se aplican a una determinada aplicación de pago:

- Las PA-DSS rigen para las aplicaciones de pago que los proveedores de software generalmente venden e instalan "en forma estándar" sin demasiada personalización.
- Las PA-DSS rigen para las aplicaciones de pago suministradas en módulos, entre los que se incluyen un módulo "base" y otros módulos específicos para funciones o tipos de clientes, o personalizados según las solicitudes de los clientes. Es posible que las PA-DSS solo se apliquen al módulo "base", cuando ese módulo es el único que realiza las funciones de pago (una vez que lo confirme un PA-QSA). Si existen otros módulos que también realizan las funciones de pago, las PA-DSS se aplicarán también a esos módulos. Tenga en cuenta que se considera una "mejor práctica" que los proveedores de software aislen las funciones de pago en un solo módulo o en pocos módulos base y, de esa manera, se puedan reservar los demás módulos para funciones que no sean de pago. Si bien no es un requisito, esta mejor práctica puede limitar la cantidad de módulos sujetos a las PA-DSS.
- Las PA-DSS no rigen para aplicaciones de pago ofrecidas por los proveedores de aplicaciones o servicios únicamente como un servicio (a menos que tales aplicaciones también sean vendidas, otorgadas bajo licencia o distribuidas a terceros) porque:
 - 1) La aplicación es un servicio que se ofrece a los clientes (normalmente comerciantes) y los clientes no tienen la posibilidad de gestionar, instalar o controlar la aplicación ni su entorno;
 - 2) La aplicación está cubierta por la propia revisión de las PCI DSS del proveedor de la aplicación o servicio (esta cobertura debe ser confirmada por el cliente);
 - 3) La aplicación no se vende, distribuye ni otorga bajo licencia a terceros.

Nota:

Los productos de aplicaciones de pago validados no deben ser versiones beta.

Algunos ejemplos de estas aplicaciones de pago de "software como servicio" son:

- 1) Las ofrecidas por los Proveedores de Servicios de Aplicaciones (ASP) que hospedan una aplicación de pago en su sitio para que la usen sus clientes. Sin embargo, tenga en cuenta que las PA-DSS regirán si la aplicación de pago del ASP también se vendiera a, y se implementara en, un sitio de terceros, y la aplicación no estuviera cubierta por la revisión de las PCI DSS del ASP.
 - 2) Las aplicaciones de terminales virtuales que residen en el sitio de los proveedores de servicios y que los comerciantes utilizan para ingresar sus transacciones de pago. Tenga en cuenta que las PA-DSS regirán si la aplicación de terminal virtual tuviera una porción que fuera distribuida a, e implementada en, el sitio del comerciante, y no estuviera cubierta por la revisión de las PCI DSS del proveedor del terminal virtual.
- "Las PA-DSS NO rigen para una aplicación de pago que se haya desarrollado para un solo cliente, o que se haya vendido a un solo cliente, dado que esta aplicación estará sujeta a la revisión normal de conformidad con las PCI DSS por parte del cliente." Tales aplicaciones (por ejemplo, una aplicación de monitorización, calificación o detección de fraude incluida en un paquete) pueden estar, pero no se exige que estén, cubiertas por las PA-DSS si todo el paquete se evalúa en conjunto. Sin embargo, si una aplicación de pago es

parte de un paquete que depende de que los controles de otras aplicaciones del paquete cumplan con los requisitos de las PA-DSS, se debe realizar una sola evaluación de las PA-DSS para la aplicación de pago y todas las demás aplicaciones del paquete en las que se apoya. Estas aplicaciones no se deben evaluar por separado de otras aplicaciones en las que se apoyan dado que todos los requisitos de las PA-DSS no se cumplen dentro de una sola aplicación.

- Las PA-DSS NO rigen para una aplicación de pago que se haya desarrollado para, y se haya vendido a, un solo cliente para ser usada exclusivamente por ese cliente, dado que esta aplicación estará sujeta a la revisión del cumplimiento normal de las PCI DSS por parte del cliente. Tenga en cuenta que tal aplicación (a la que se puede denominar aplicación "personalizada") se vende a un solo cliente (por lo general, un gran comerciante o proveedor de servicios), y está diseñada y desarrollada según las especificaciones provistas por el cliente.
- Las PA-DSS NO rigen para aplicaciones de pago desarrolladas por comerciantes y proveedores de servicios si solo se utilizan internamente (no se venden, no se distribuyen ni se otorgan bajo licencia a terceros), dado que estas aplicaciones de uso interno deberían estar sujetas al cumplimiento normal de las PCI DSS por parte de los comerciantes o proveedores de servicios.

Por ejemplo, para estos dos últimos casos, el hecho de que la aplicación de pago desarrollada para uso interno o "personalizada" almacene datos confidenciales de autenticación prohibidos o permita contraseñas complejas se consideraría como parte de los esfuerzos de cumplimiento normal de las PCI DSS realizados por el comerciante o el proveedor de servicios y no requeriría un evaluación de las PA-DSS por separado.

La siguiente lista, si bien no es del todo exhaustiva, detalla las aplicaciones que NO se consideran aplicaciones de pago a los fines de las PA-DSS (y, por lo tanto, no necesitan ser sometidas a revisiones según las PA-DSS):

- Sistemas operativos en los que se instala una aplicación de pago (por ejemplo, Windows, Unix).
- Sistemas de bases de datos que almacenan información de titulares de tarjetas (por ejemplo, Oracle).
- Sistemas de gestión operativa que almacenan datos de titulares de tarjetas (por ejemplo, para elaboración de informes o servicio al cliente).

Nota: El PCI SSC SÓLO especificará aplicaciones que sean aplicaciones de pago.

El alcance de la revisión según las PA-DSS debe incluir lo siguiente:

- Cobertura de todas las funciones de la aplicación de pago, incluidas, entre otras, 1) las funciones de pago completas (autorización y liquidación), 2) las entradas y las salidas de datos, 3) los estados de error, 4) las interfaces y las conexiones con otros archivos, sistemas y/o aplicaciones de pago o componentes de la aplicación, 5) todos los flujos de datos del titular de la tarjeta, 6) los mecanismos de cifrado y 7) los mecanismos de autenticación.
- Cobertura del asesoramiento que el proveedor de aplicaciones de pago debe brindarles a los clientes y a los revendedores/integradores (consulte la *Guía de implementación de las PA-DSS* más adelante en este documento) para asegurar que: 1) el cliente sepa cómo implementar la aplicación de pago a fin de que cumpla con la PCI DSS, y 2) se le diga al cliente con claridad que determinadas configuraciones del entorno y de la aplicación de pago pueden impedir que se cumpla con las PCI DSS. Tenga en cuenta que es posible que el proveedor de aplicaciones de pago tenga que brindar ese asesoramiento incluso cuando la configuración específica: 1) no pueda ser controlada por el proveedor de aplicaciones de pago una vez que el cliente haya instalado la aplicación o 2) sea responsabilidad del cliente y no del proveedor de aplicaciones de pago.

- Cobertura de todas las plataformas seleccionadas para la aplicación de pago revisada (se deben especificar las plataformas incluidas).
- Cobertura de las herramientas utilizadas por la aplicación de pago, o dentro de ella, para acceder y/o visualizar los datos de titulares de tarjetas (herramientas de información, de registro, etc.)

Aplicabilidad de las PA-DSS a las aplicaciones de pago en terminales de hardware

Las aplicaciones de pago diseñadas para funcionar en terminales de hardware (también conocidos como terminal POS autónomo o dedicado) pueden ser sometidas a una revisión según las PA-DSS si el proveedor desea obtener validación y se puede cumplir con los requisitos de cumplimiento de las PA-DSS. Las razones por las que es posible que un proveedor desee someter una aplicación de pago en un terminal de hardware a una validación según las PA-DSS incluyen, entre otras, las necesidades del negocio y las obligaciones de cumplimiento. Esta sección proporciona asesoramiento para los proveedores que deseen obtener validación según las PA-DSS para aplicaciones de pago residentes en terminales de hardware.

Existen dos maneras de que una aplicación de pago residente en un terminal de hardware obtenga validación según las PA-DSS:

1. La aplicación de pago residente cumple directamente con todos los requisitos de las PA-DSS y es validada de acuerdo con los procedimientos estándar de las PA-DSS.
2. La aplicación de pago residente no cumple con todos los requisitos de las PA-DSS, pero el hardware en que reside la aplicación está incluido en la Lista de Dispositivos Aprobados de Seguridad de Transacciones con PIN (PTS) del PCI SSC como un dispositivo de Punto de Interacción (POI) actualmente aprobado por PCI PTS. En este escenario, es posible que la aplicación cumpla con los requisitos de las PA-DSS mediante una combinación de los controles validados por las PA-DSS y PTS.

El resto de esta sección sólo rige para las aplicaciones de pago que residan en un dispositivo POI validado que haya sido aprobado por PCI PTS. Si la aplicación de pago no puede cumplir directamente con uno o más de los requisitos de las PA-DSS, éstos se pueden satisfacer indirectamente mediante controles probados como parte de la validación de PCI PTS. Para que se considere la inclusión de un dispositivo de hardware en una revisión según las PA-DSS, el dispositivo DEBE ser validado como un dispositivo POI aprobado por PCI PTS y estar incluido en la Lista de Dispositivos PTS Aprobados del PCI SSC. El dispositivo POI con validación PTS, que proporciona un entorno de informática confiable, será una “**dependencia obligatoria**” para la aplicación de pago, y la combinación de aplicación y hardware aparecerá en la Lista de Aplicaciones de Pago Validadas de las PA-DSS.

Al realizar la evaluación de las PA-DSS, el PA-QSA debe probar completamente la aplicación de pago con su hardware dependiente con respecto a todos los requisitos de las PA-DSS. Si el PA-QSA determina que la aplicación de pago residente no puede cumplir con uno o más requisitos de las PA-DSS, pero que éstos se satisfacen mediante el uso de controles validados conforme a PCI PTS, el PA-QSA debe:

1. Documentar claramente cuáles requisitos se cumplen de conformidad con las PA-DSS (como de costumbre);
2. Documentar claramente cuál requisito se cumplió mediante PCI PTS en la casilla “Implementado” de ese requisito;
3. Incluir una explicación detallada de por qué la aplicación de pago no pudo cumplir con los requisitos de las PA-DSS;
4. Documentar los procedimientos que se realizaron para determinar cómo se cumplió plenamente con ese requisito a través de un control validado por PCI PTS;

5. Especificar el terminal de hardware validado por PCI PTS como una dependencia obligatoria en el Resumen ejecutivo del Informe de validación.

Una vez que el PA-QSA complete la validación de la aplicación de pago y sea consecuentemente aceptada por el PCI SSC, el dispositivo de hardware validado por PTS se especificará como un dependencia para la aplicación de pago en la Lista de Aplicaciones Validadas de las PA-DSS.

Las aplicaciones de pago residentes en terminales de hardware que sean validadas a través de una combinación de controles PA-DSS y PCI PTS deben cumplir con los siguientes criterios:

1. Ser proporcionadas al cliente como una unidad (terminal de hardware y aplicación) O, si se proporcionan por separado, el proveedor de la aplicación y/o el revendedor/integrador debe empaquetar la aplicación para su distribución de tal modo que ésta funcione solamente en el terminal de hardware en el que se validó su ejecución.
2. Activadas de forma predeterminada para respaldar el cumplimiento de las PCI DSS por parte del cliente.
3. Incluir asistencia técnica constante y actualizaciones para mantener el cumplimiento de las PCI DSS.
4. Si la aplicación se vende, distribuye u otorga bajo licencia a los clientes por separado, el proveedor debe proporcionar los detalles del hardware dependiente que se debe usar con la aplicación, de acuerdo con lo especificado en la validación según las PA-DSS.

Funciones y responsabilidades

A continuación, se definen las funciones y las responsabilidades de las partes interesadas en la comunidad de las aplicaciones de pago. Algunas de estas partes interesadas tienen una participación más directa en el proceso de evaluación de las PA-DSS, como los proveedores, los PA-QSA y el PCI SSC. Otras partes interesadas que no se encuentran directamente involucradas en el proceso de evaluación deben conocer todo el proceso para que la toma de decisiones comerciales relacionadas les resulte más fácil.

A continuación, se definen las funciones y las responsabilidades de las partes interesadas en la comunidad de las aplicaciones de pago. Las responsabilidades correspondientes a las partes interesadas que están involucradas en el proceso de evaluación se indican en una lista.

Marcas de pago

American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. son las marcas de pago que fundaron el PCI SSC. Estas marcas de pago son responsables de desarrollar y aplicar los programas relacionados con el cumplimiento de las PA-DSS, que incluyen, pero no se limitan a, lo siguiente:

- Los requisitos, los mandatos o las fechas para el uso de las aplicaciones de pago que cumplen con lo establecido en las PA-DSS
- Las multas o las sanciones relacionadas con el uso de aplicaciones de pago que no cumplen con lo establecido en las PA-DSS

Las marcas de pago pueden definir programas de cumplimiento, mandatos, fechas, etc., mediante el uso de las PA-DSS y las aplicaciones de pago validadas que el PCI SSC especifica. Mediante estos programas de cumplimiento, las marcas de pago promocionan el uso de las aplicaciones de pago validadas que se especifican.

Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC)

El PCI SSC es el ente regulador que preserva las normas de la industria de tarjetas de pago, incluidas la PCI DSS y las PA-DSS. En relación con las PA-DSS, las PCI SSC:

- Forman un registro centralizado para los informes de validación (ROV) según las PA-DSS.
- Realiza revisiones de control de calidad (QA) de los informes de validación según las PA-DSS para confirmar la coherencia y la calidad de los informes.
- Especifica en el sitio web las aplicaciones de pago validadas según las PA-DSS.
- Autoriza y capacita a los PA-QSA para que realicen revisiones según las PA-DSS.
- Mantiene y actualiza las PA-DSS y la documentación relacionada de acuerdo con un proceso de administración del ciclo de vida de las normas

Tenga en cuenta que el PCI SSC no aprueba informes desde una perspectiva de validación. La función del PA-QSA es documentar el cumplimiento de las aplicaciones de pago con las PA-DSS a la fecha de la evaluación. Asimismo, el PCI SSC realiza un QA para garantizar que el PA-QSA documente de manera precisa y completa las evaluaciones de las PA-DSS.

Proveedores de software

Los proveedores de software (“proveedores”) desarrollan aplicaciones de pago que almacenan, procesan o transmiten datos de titulares de tarjetas como parte de la autorización o de la liquidación y, luego, venden, distribuyen u otorgan estas aplicaciones de pago bajo licencia a terceros (clientes o revendedores/integradores). Los proveedores son responsables de:

- Crear aplicaciones de pago conformes con las PA-DSS que faciliten, y no entorpezcan, el cumplimiento de las PCI DSS por parte de los clientes (la aplicación no puede requerir una implementación ni parámetros de configuración que violen un requisito de las PCI DSS).
- Cumplir con los requisitos de las PCI DSS cada vez que el proveedor almacene, procese o transmita datos de titulares de tarjetas (por ejemplo, durante la resolución de problemas del cliente).
- Crear una *Guía de implementación de las PA-DSS*, específica para cada aplicación de pago, según los requisitos establecidos en este documento.
- Educar a los clientes, revendedores e integradores acerca de cómo instalar y configurar las aplicaciones de pago de conformidad con las PCI DSS.
- Asegurar que las aplicaciones de pago cumplan con las PA-DSS y que aprueben satisfactoriamente una revisión según las PA-DSS, como se especifica en el presente documento.

PA-QSA

Los PA-QSA son QSA que han recibido la certificación y la capacitación del PCI SSC para realizar revisiones según las PA-DSS.

Los PA-QSA son responsables de:

- Realizar evaluaciones de las aplicaciones de pago de acuerdo con los Procedimientos de Evaluación de Seguridad y los Requisitos de Validación del PA-QSA.
- Proporcionar una opinión en cuanto a si la aplicación de pago satisface los requisitos de las PA-DSS.
- Proporcionar la documentación adecuada en el ROV para demostrar que la aplicación de pago cumple con las PA-DSS.
- Presentar el ROV al PCI SSC, junto con la Declaración de validación (firmada por el PA-QSA y el proveedor).
- Mantener un proceso interno de control de calidad para las tareas de su PA-QSA.

Nota: Tenga en cuenta que no todos los QSA son PA-QSA. El QSA debe cumplir con requisitos de calificación adicionales para poder ser un PA-QSA.

Es responsabilidad del PA-QSA declarar si la aplicación de pago logró la debida conformidad. El PCI SSC no aprueba los ROV desde una perspectiva de cumplimiento técnico, sino que realiza revisiones de QA en los informes de validación para garantizar que los informes documenten de manera adecuada la evidencia de cumplimiento.

Revendedores e integradores

Los revendedores e integradores son entidades que venden, instalan o reparan aplicaciones de pago en representación de proveedores de software u otros. Los revendedores y los integradores son responsables de:

- Implementar una aplicación de pago que cumpla las PA-DSS dentro de un entorno que, a la vez, respete las PCI DSS (o debe instruir al comerciante para que lo haga).
- Configurar la aplicación de pago (cuando se proporcionen opciones de configuración) de acuerdo con la *Guía de implementación de las PA-DSS* suministrada por el proveedor.
- Configurar la aplicación de pago (o instruir al comerciante para que lo haga) de conformidad con las PCI DSS.
- Realizar el servicio técnico de las aplicaciones de pago (por ejemplo, resolución de problemas, entrega de actualizaciones remotas y prestación de asistencia remota) de acuerdo con la *Guía de implementación de las PA-DSS* y la PCI DSS.

Los revendedores e integradores no presentan aplicaciones de pago para su evaluación. Únicamente los proveedores pueden presentar productos.

Cientes

Los clientes son comerciantes, proveedores de servicios u otras personas que compran o reciben la aplicación de pago de un tercero con el fin de almacenar, procesar o transmitir datos de titulares de tarjetas como parte de una autorización o liquidación de transacciones de pago. Los clientes que desean utilizar aplicaciones que cumplan con las PA-DSS son responsables de:

- Implementar una aplicación de pago que cumpla las PA-DSS dentro de un entorno que, a la vez, respete las PCI DSS.
- Configurar la aplicación de pago (cuando se proporcionen opciones de configuración) de acuerdo con la *Guía de implementación de las PA-DSS* suministrada por el proveedor.
- Configurar la aplicación de pago de conformidad con las PCI DSS.
- Mantener el estado de cumplimiento de las PCI DSS tanto para el entorno como para la configuración de la aplicación de pago.

Nota: Una aplicación de pago que cumpla únicamente con las PA-DSS no garantiza el cumplimiento de las PCI DSS.

Guía de implementación de las PA-DSS

Las aplicaciones de pago validadas se deben poder implementar de conformidad con las PCI DSS. Los proveedores de software deben proporcionar una *Guía de implementación de las PA-DSS* para instruir a sus clientes y revendedores/integradores sobre la implementación de un producto seguro, documentar los detalles específicos de configuración segura mencionados en este documento, así como delinear claramente las responsabilidades del proveedor, el revendedor/integrador y el cliente en el cumplimiento de los requisitos de las PCI DSS. Esta guía debe detallar la manera en que el cliente y/o el revendedor/integrador debería activar los valores de configuración de seguridad dentro de la red del cliente. Por ejemplo, la *Guía de implementación de las PA-DSS* debe considerar las responsabilidades y las características básicas de seguridad de la contraseña de las PCI DSS aun cuando no esté controlada por la aplicación de pago, a fin de que el cliente o el revendedor/integrador pueda entender cómo implementar contraseñas seguras para cumplir con las PCI DSS.

Las aplicaciones de pago, cuando se implementan según la *Guía de implementación de las PA-DSS* y en un entorno que cumpla con las PCI DSS, deben facilitar y respaldar el cumplimiento de las PCI DSS por parte de los clientes.

Consulte el *Anexo A: Resumen del contenido de la Guía de implementación de las PA-DSS* para comparar las responsabilidades de implementación de los controles que se especifican en la *guía*.

Requisitos del Asesor de Seguridad Certificado para las Aplicaciones de Pago (PA-QSA)

Únicamente los Asesores de Seguridad Certificados para las Aplicaciones de Pago (PA-QSA) empleados por las empresas de Asesores de Seguridad Certificados (QSA) están autorizados para realizar las evaluaciones de las PA-DSS. Para una lista de empresas calificadas para realizar evaluaciones de las PA-DSS, consulte la Lista de Asesores de Seguridad Certificados en www.pcisecuritystandards.org.

- El PA-QSA debe utilizar los procedimientos de pruebas detallados en este documento acerca de las Normas de Seguridad de Datos para las Aplicaciones de Pago.
- El PA-QSA debe tener acceso al laboratorio donde se llevará a cabo el proceso de validación.

Laboratorio de pruebas

- Los laboratorios de pruebas pueden estar en uno de dos lugares: en la ubicación del PA-QSA o en la ubicación del proveedor de software.
- Este laboratorio debe poder simular el uso real de la aplicación de pago.
- El PA-QSA debe validar la instalación adecuada del entorno de laboratorio para asegurarse de que éste simule fielmente una situación real y que el proveedor no haya modificado o alterado el entorno de ninguna manera.
- Consulte el *Anexo B: Confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS* que aparece en este documento si desea ver los requisitos detallados de los procesos de laboratorio y los procesos relacionados.
- El PA-QSA debe llenar y presentar el *Anexo B*, según el laboratorio específico utilizado para la aplicación de pago que está siendo revisada, como parte del informe completo de las PA-DSS.

Información sobre la aplicabilidad de las PCI DSS

(Extraído de las PCI DSS)

Las *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago* (PCI DSS) se aplica cada vez se almacenan, procesan o transmiten datos de cuentas. Los datos de cuentas constan de los datos de titulares de cuentas más datos confidenciales de autenticación, como se detalla a continuación.

Los datos de titulares de cuentas incluyen:	Los datos confidenciales de autenticación incluyen:
<ul style="list-style-type: none">▪ Número de cuenta principal (PAN)▪ Nombre del titular de la tarjeta▪ Fecha de vencimiento▪ Código de servicio	<ul style="list-style-type: none">▪ Todos los datos de la banda magnética o datos equivalentes que están en un chip▪ CAV2/CVC2/CVV2/CID▪ PIN/Bloqueos de PIN

El número de cuenta principal (PAN) es el factor que define la aplicabilidad de los requisitos de las PCI DSS y las PA-DSS. Los requisitos de las PCI DSS se aplican si se almacena, procesa o transmite un número de cuenta principal (PAN). Si no se almacena, procesa ni transmite el PAN, no se aplicarán las PCI DSS ni las PA-DSS.

Si el nombre del titular de la tarjeta, el código de servicio y/o la fecha de vencimiento no se almacenan, procesan ni transmiten con el PAN, ni están presentes de alguna otra manera en el entorno de datos de titulares de tarjeta, se deben proteger de acuerdo con todos los requisitos de las PCI DSS, **a excepción de** los Requisitos 3.3 y 3.4, que sólo se aplican al PAN.

Las PCI DSS representan un conjunto mínimo de objetivos de control que puede ser reforzado con leyes y regulaciones locales, regionales y sectoriales. Además, la legislación o las regulaciones puede requerir protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de la tarjeta), o definir las prácticas de divulgación de una entidad en lo que respecta a las información de los consumidores. Entre los ejemplos está la legislación relacionada con la protección de los datos de los consumidores, la privacidad, el robo de identidad o la seguridad de los datos. Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones del gobierno ni otros requisitos legales.

La siguiente tabla de las *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago* (PCI DSS) ilustra los elementos que habitualmente se utilizan de los datos de titulares de tarjetas y los datos confidenciales de autenticación, independientemente de que esté permitido o prohibido el **almacenamiento** de dichos datos o de que esos datos deban estar **protegidos**. Esta tabla no pretende ser exhaustiva, pero se proporciona con el fin de ilustrar distintos tipos de requisitos que se le aplican a cada elemento de datos.

		Elemento de datos	Almacenamiento permitido	Hace que los datos de la cuenta almacenados no se puedan leer según el Requisito 3.4 de las PCI DSS
Datos de la cuenta	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación ¹	Datos completos de la banda magnética ²	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN	No	No se pueden almacenar según el Requisito 3.2

Los Requisitos 3.3 y 3.4 de las PCI DSS sólo se aplican al PAN. Si el PAN se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN debe ser ilegible de acuerdo con el Requisito 3.4 de las PCI DSS.

Las PCI DSS **sólo se aplican** si los PAN se almacenan, procesan y/o transmiten.

¹ No se deben almacenar los datos confidenciales de autenticación después de la autorización (incluso si están cifrados).

² Contenido completo de la pista de banda magnética, datos equivalentes que están en el chip o en cualquier otro dispositivo.

Instrucciones y contenido para el informe de validación

Los PA-QSA utilizarán este documento como plantilla para crear el Informe de validación. En el momento de completar un Informe de validación, todos los PA-QSA deben seguir las instrucciones establecidas en el documento respecto del contenido y el formato del informe.

El Informe de validación debe contener la siguiente información como prefacio de los Requisitos y Procedimientos de Evaluación de Seguridad:

1. Descripción del alcance de la revisión

- Describa el alcance de la cobertura de la revisión, según la sección anterior sobre el Alcance de las PA-DSS.
- Plazo de validación.
- Versión de las PA-DSS utilizada para la evaluación
- Lista de la documentación revisada

2. Resumen ejecutivo

Incluya lo siguiente:

- Nombre del producto.
- Versión del producto y plataformas afines consideradas.
- Lista de revendedores o integradores para este producto.
- Sistemas operativos con que se probó la aplicación de pago.
- Software de base de datos que utilizó o admitió la aplicación de pago.
- Breve descripción de la aplicación de pago o de la familia de productos (2 ó 3 oraciones).
- Diagrama de red de una implementación típica de la aplicación de pago (no es necesario que sea una implementación específica que esté en el sitio de un cliente) que incluya, de la manera más detallada posible, lo siguiente:
 - Las conexiones de entrada y salida de la red del cliente.
 - Los componentes que hay dentro de la red del cliente, incluidos los dispositivos POS, los sistemas, las bases de datos y los servidores web según corresponda.
 - Otras aplicaciones de pago o componentes necesarios, según corresponda.
- Descripción o diagrama de cada segmento del enlace de comunicaciones, incluidos (1) LAN, WAN o Internet, (2) comunicación de software de host a host y (3) dentro del host donde se implementa el software (por ejemplo, de qué manera dos procesos diferentes se comunican entre sí en el mismo host).
- Un diagrama de flujo de datos que muestre todos los flujos de datos de titulares de tarjetas, incluida la autorización, la captura, la liquidación y los flujos de reintegros de cobros, según corresponda.

- Breve descripción de los archivos y las tablas que almacenan datos de titulares de tarjetas, respaldados por un inventario creado (u obtenido del proveedor de software) y retenido por el PA-QSA en los documentos de trabajo. Para cada almacenamiento (archivo, tabla, etc.) de datos de titulares de tarjetas, este inventario debe incluir:
 - Una lista de todos los elementos correspondientes a los datos almacenados de los titulares de tarjetas.
 - Cómo se asegura el almacenamiento de datos.
 - Cómo se registra el acceso al almacenamiento de datos.
- Una lista de todos los componentes de software relacionados con la aplicación de pago, incluidos los requisitos y las dependencias de software de terceros.
- Una descripción de los métodos de autenticación completos de la aplicación de pago, incluido el mecanismo de autenticación de la aplicación, la base de datos de autenticación y la seguridad del almacenamiento de datos.
- Una descripción de la función de la aplicación de pago en una implementación típica y cuáles son los otros tipos de aplicaciones de pago necesarios para una implementación de pago completa.
- Una descripción del cliente típico al que se le venderá este producto (por ejemplo, una empresa grande o pequeña, ya sea específica de la industria, de Internet o con instalaciones físicas) y la base de clientes del proveedor (por ejemplo, segmento del mercado, nombres de grandes clientes).
- Definición de la metodología de control de versiones del proveedor para describir/ilustrar cómo indica el proveedor los cambios de versión importantes y menores por medio de números de versión, y para definir qué tipos de cambios incluye el proveedor en los cambios de versión importantes y menores.

Nota: Anexo B: Una confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS también se debe completar y presentar junto con el informe completo de las PA-DSS.

3. Conclusiones y observaciones

- Todos los PA-QSA deben utilizar la siguiente plantilla para proporcionar descripciones y conclusiones detalladas del informe.
- Describa las pruebas realizadas que no se hayan incluido en la columna de procedimientos de prueba.
- Si el evaluador determina que un requisito no se puede aplicar para una aplicación de pago dada, se debe incluir una explicación en la columna “Implementado” de ese requisito.

4. Información de contacto y fecha del informe

- Información de contacto del proveedor de software (incluida la dirección URL, el número de teléfono y la dirección de correo electrónico).
- Información de contacto del PA-QSA (incluido el nombre, el número de teléfono y la dirección de correo electrónico).
- Información del contacto principal de control de calidad (QA) del PA-QSA (incluido el nombre del contacto principal de QA, el número de teléfono y la dirección de correo electrónico).
- Fecha del informe

Pasos para completar las PA-DSS

El presente documento contiene la tabla de Requisitos y Procedimientos de Evaluación de Seguridad, así como el *Anexo B: Confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS*. Los Requisitos y Procedimientos de Evaluación de Seguridad detallan los procedimientos que debe seguir el PA-QSA. El *Anexo B: El PA-QSA debe completar una confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS* para confirmar el estado y las capacidades del laboratorio de pruebas que se utilizarán para realizar la evaluación de las PA-DSS.

El PA-QSA debe realizar lo siguiente:

1. Completar el informe de validación y utilizar el presente documento como plantilla.
 - a. Completar el prefacio del informe de validación, de acuerdo con la sección titulada “Instrucciones y contenido del informe de validación”.
 - b. Completar y documentar todos los pasos detallados en los Procedimientos de Evaluación de Seguridad, incluidas las breves descripciones de los controles observados en la columna “Implementado”, y anotar los comentarios necesarios. *Tenga en cuenta que un informe que contenga opiniones en la columna “No implementado” no se debe presentar ante el PCI SSC hasta que todos los elementos figuren en “Implementado”.*
2. Completar el *Anexo B: Confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS*.
3. Completar y firmar una *Declaración de validación* (el PA-QSA y el proveedor de software). La Declaración de validación está disponible en el sitio web del PCI SSC (www.pcisecuritystandards.org).
4. Una vez completos, presente todos los documentos mencionados anteriormente ante el PCI SSC de acuerdo con la *Guía del programa PA-DSS*.

Guía del programa PA-DSS

Consulte la *Guía del programa PA-DSS* para obtener información sobre la gestión del programa de las PA-DSS, incluidos los siguientes temas:

- Procesos de presentación y aceptación del informe de PA-DSS.
- Proceso de renovación anual para las aplicaciones de pago incluidas en la Lista de aplicaciones validadas según las PA-DSS.
- Transición de las aplicaciones validadas según las PABP a la lista de aplicaciones de pago validadas según las PA-DSS.
- Responsabilidades de notificación en caso de que se determine que una aplicación de pago publicada no cumple con algún compromiso.

El PCI SSC se reserva el derecho de requerir una revalidación por cambios significativos en las Normas de Seguridad de Datos para las Aplicaciones de Pago y/o por vulnerabilidades identificadas específicamente en una aplicación de pago publicada.

Requisitos y procedimientos de evaluación de seguridad de las PA-DSS

Requisitos de las PA-DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1. No retenga toda la banda magnética, el código o valor de validación de la tarjeta (CAV2, CID, CVC2, CVV2), ni los datos de bloqueo del PIN.				
<p>1.1 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 1.1.1 a 1.1.3 establecidos a continuación.</p> <p>Notas:</p> <ul style="list-style-type: none"> ▪ <i>Al prohibir el almacenamiento de datos confidenciales de autenticación después de la autorización, se considera que la transacción completó el proceso de autorización y que el cliente recibió la aprobación definitiva de la transacción. Una vez completa la autorización, no se podrán almacenar estos datos confidenciales de autenticación.</i> ▪ <i>Es posible que los emisores de tarjetas de pago y las empresas que respaldan los servicios de emisión almacenen datos confidenciales de autenticación si existe una justificación de negocio y los datos están almacenados de forma segura.</i> <p>Concuerda con el Requisito 3.2 de las PCI DSS</p>	<p>1.1.a Si esta aplicación de pago almacena información confidencial de autenticación, verifique que la aplicación sea solamente para emisores de tarjetas de pago y/o empresas que respaldan los servicios de emisión.</p>			
	<p>1.1.b Para todas las demás aplicaciones de pago, si los datos confidenciales de autenticación (ver 1.1.1–1.1.3 abajo) se almacenan antes de la autorización y luego se eliminan, obtenga y revise la metodología para eliminar los datos a fin de determinar que sean irre recuperables.</p>			
	<p>1.1.c Para cada rubro de datos confidenciales de autenticación que aparece a continuación, realice los siguientes pasos una vez que haya completado las numerosas transacciones de prueba que simulan todas las funciones de la aplicación de pago, a fin de incluir la generación de todas las condiciones de error y las entradas de registro.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
<p>1.1.1 Después de la autorización, no almacene contenidos completos de ninguna pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo). Estos datos se denominan alternativamente pista completa, pista, pista 1, pista 2 y datos de banda magnética.</p> <p>Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:</p> <ul style="list-style-type: none"> ▪ El nombre del titular de la cuenta. ▪ Número de cuenta principal (PAN). ▪ Fecha de vencimiento. ▪ Código de servicio. <p>Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.</p> <p>Concuerda con el Requisito 3.2.1 de las PCI DSS</p>	<p>1.1.1 Utilice las herramientas y/o métodos forenses (herramientas comerciales, secuencias de comandos, etc.)³ para examinar todos los resultados creados por la aplicación de pago y verificar que todo el contenido de cualquier pista de la banda magnética en el reverso de la tarjeta o datos equivalentes que estén en un chip no sean almacenados después de la autorización. Incluya por lo menos los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago):</p> <ul style="list-style-type: none"> ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Memoria no volátil, incluida la memoria caché no volátil ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos 			

³ Herramienta o método forense: Herramienta o método para descubrir, analizar y presentar datos forenses, que brinda una manera sólida de autenticar, buscar y recuperar evidencia informática con rapidez y de modo exhaustivo. En el caso de las herramientas o los métodos forenses que utilizan los PA-QSA, tales herramientas o métodos deben localizar con precisión los datos confidenciales de autenticación escritos por la aplicación de pago. Estas herramientas pueden ser comerciales, de código abierto o desarrolladas para uso interno por el PA-QSA.

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>1.1.2 Después de la autorización, no almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes.</p> <p>Concuerda con el Requisito 3.2.2 de las PCI DSS</p>	<p>1.1.2 Utilice las herramientas y/o métodos forenses (herramientas comerciales, secuencias de comandos, etc.) para examinar los resultados creados por la aplicación de pago y verificar que el código de validación de la tarjeta de tres o cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no quede almacenado después de la autorización. Incluya por lo menos los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago):</p> <ul style="list-style-type: none"> ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Memoria no volátil, incluida la memoria caché no volátil ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos 			
<p>1.1.3 Después de la autorización, no almacene el número de identificación personal (PIN) ni el bloqueo de PIN cifrado.</p> <p>Concuerda con el Requisito 3.2.3 de las PCI DSS</p>	<p>1.1.3 Utilice las herramientas y/o métodos forenses (herramientas comerciales, secuencia de comandos, etc.) para examinar los resultados creados por la aplicación de pago y comprobar que los PIN y los bloqueos de PIN cifrados no queden almacenados después de la autorización. Incluya por lo menos los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago).</p> <ul style="list-style-type: none"> ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Memoria no volátil, incluida la memoria caché no volátil ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos 			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>1.1.4 Borre de manera segura los datos que haya en la banda magnética, los valores o los códigos de validación de la tarjeta y los PIN o los datos de bloqueo de PIN almacenados por versiones anteriores de la aplicación de pago, de acuerdo con las normas aceptadas de la industria para una eliminación segura y según se define, por ejemplo, en la lista de productos aprobados de la Agencia de Seguridad Nacional u otra norma o reglamentación estatal o nacional.</p> <p><i>Nota: Este requisito solamente se implementa cuando existen versiones anteriores de la aplicación de pago que hayan almacenado datos confidenciales de autenticación.</i></p> <p>Concuerda con el Requisito 3.2 de las PCI DSS</p>	<p>1.1.4.a Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores:</p> <ul style="list-style-type: none"> ▪ Que se deben eliminar los datos históricos (datos de la banda magnética, códigos de validación de la tarjeta, PIN o bloqueos de PIN almacenados por versiones anteriores de la aplicación de pago). ▪ Cómo eliminar los datos históricos. ▪ Que dicha eliminación es absolutamente necesaria para cumplir las PCI DSS. <p>1.1.4.b Verifique que el proveedor proporcione una herramienta o un procedimiento de limpieza seguro para eliminar los datos.</p> <p>1.1.4.c Verifique que, mediante el uso de herramientas y/o métodos forenses, la herramienta o procedimiento de limpieza seguro proporcionado por el proveedor elimine los datos de manera segura, de acuerdo con las normas aceptadas en la industria para la eliminación segura de datos.</p>			
<p>1.1.5 Borre de manera segura los datos confidenciales de autenticación (datos previos a la autorización) que se utilizan con fines de depuración o resolución de problemas desde los archivos de registro, los archivos de depuración y otras fuentes de datos que se reciben de los clientes, a fin de asegurar que los datos de banda magnética, los códigos o valores de validación de la tarjeta y los PIN o los datos de bloqueo de PIN no queden almacenados en los sistemas del proveedor de software. Estas fuentes de datos se deben recopilar en cantidades limitadas y sólo cuando sea necesario para resolver un problema, se deben cifrar cuando se almacenan y se deben borrar inmediatamente después de ser utilizadas.</p> <p>Concuerda con el Requisito 3.2 de las PCI DSS</p>	<p>1.1.5.a Examine los procedimientos del proveedor del software para resolver problemas de los clientes y compruebe que los procedimientos incluyan:</p> <ul style="list-style-type: none"> ▪ Recopilación de datos confidenciales de autenticación sólo cuando sea necesario para resolver un problema específico. ▪ Almacenamiento de dichos datos en ubicaciones específicas y conocidas que tengan acceso limitado. ▪ Recopilación de una cantidad limitada de datos necesarios para resolver un problema específico. ▪ Cifrado de los datos confidenciales de autenticación cuando se almacenen. ▪ Borrado seguro de dichos datos inmediatamente después de utilizarlos. <p>1.1.5.b Seleccione una muestra de solicitudes recientes de resolución de problemas presentadas por los clientes, y compruebe que cada evento siguió el procedimiento examinado en 1.1.5.a.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
	<p>1.1.5.c Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores:</p> <ul style="list-style-type: none"> ▪ Recopilar datos confidenciales de autenticación sólo cuando sea necesario para resolver un problema específico. ▪ Almacenar dichos datos en ubicaciones específicas y conocidas que tengan acceso limitado. ▪ Recopilar sólo los datos confidenciales de autenticación que sean necesarios para resolver un problema específico. ▪ Cifrar los datos confidenciales de autenticación mientras estén almacenados. ▪ Borrar de manera segura dichos datos inmediatamente después de utilizarlos. 			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
2. Proteja los datos del titular de la tarjeta que fueron almacenados				
<p>2.1 El proveedor de software debe asesorar a los clientes sobre cómo purgar los datos del titular de la tarjeta después de que haya caducado el período de retención definido por el cliente.</p> <p>Concuerda con el Requisito 3.1 de las PCI DSS</p>	<p>2.1 Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que la documentación incluya la siguiente orientación para los clientes y los revendedores/integradores:</p> <ul style="list-style-type: none"> ▪ Se deben purgar los datos del titular de la tarjeta que excedan el período de retención definido por el cliente. ▪ Una lista de todas las ubicaciones donde la aplicación de pago almacena datos de los titulares de tarjeta (para que el cliente sepa las ubicaciones de los datos que se deben eliminar). ▪ Instrucciones para configurar el software o los sistemas subyacentes (como el sistema operativo, bases de datos, etc.) para impedir la captura o retención involuntaria de datos del titular de la tarjeta. Por ejemplo, puntos de copia de seguridad y restauración del sistema. 			
<p>2.2 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).</p> <p>Notas:</p> <ul style="list-style-type: none"> ▪ <i>Este requisito no se aplica a aquellos empleados y otras partes que tengan una necesidad de negocio válida para ver el PAN completo.</i> ▪ <i>Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]).</i> <p>Concuerda con el Requisito 3.3 de las PCI DSS</p>	<p>2.2 Revise las vistas de datos de tarjetas de crédito, incluidos, por ejemplo, los dispositivos POS, las pantallas, los registros y los recibos, para determinar que los números de tarjeta de crédito se oculten en el momento de visualizar los datos del titular de la tarjeta, salvo para quienes necesiten ver los números de tarjeta de crédito completos por razones de negocio.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>2.3 Haga que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos:</p> <ul style="list-style-type: none"> ▪ Valores hash de una vía basados en criptografía sólida (el hash debe ser de todo el PAN). ▪ Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) ▪ Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). ▪ Criptografía sólida con procesos y procedimientos asociados para la gestión de claves. <p>Notas:</p> <ul style="list-style-type: none"> ▪ <i>Para una persona maliciosa sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si una aplicación de pago genera versiones en valores hash y truncada del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncada no se puedan correlacionar para reconstruir el PAN original.</i> ▪ <i>Se debe dejar ilegible el PAN en todo lugar donde se almacene, incluso fuera de la aplicación de pago.</i> <p>Concuerda con el Requisito 3.4 de las PCI DSS</p>	<p>2.3 Compruebe que el PAN quede ilegible en todo lugar donde se almacene, de la siguiente manera.</p>			
	<p>2.3.a Examine el método utilizado para proteger el PAN, incluidos los algoritmos de cifrado (si corresponde). Verifique que el PAN quede ilegible mediante el uso de uno de los siguientes métodos:</p> <ul style="list-style-type: none"> ▪ Valores hash de una vía en criptografía sólida. ▪ Truncamiento. ▪ Token y ensambladores de índices (los ensambladores se deben almacenar de manera segura). ▪ Criptografía sólida, con procesos y procedimientos relacionados de gestión de claves. 			
	<p>2.3.b Examine varias tablas o archivos de los depósitos de datos creados o generados por la aplicación para verificar que el PAN quede ilegible.</p>			
	<p>2.3.c Si la aplicación crea o genera archivos para ser utilizados fuera de la aplicación (por ejemplo, archivos generados para exportación o copias de seguridad), incluso para almacenamiento en medios removibles, examine una muestra de los archivos generados, incluidos los generados en medios removibles (por ejemplo, cintas de copias de seguridad), para confirmar que el PAN queda ilegible.</p>			
	<p>2.3.d Examine una muestra de los archivos de auditoría creados o generados por la aplicación para confirmar que el PAN queda ilegible o es eliminado de los registros.</p>			
<p>2.3.e Si el proveedor de software almacena el PAN por alguna razón (por ejemplo, porque se recibieron de parte de los clientes archivos de registro, de depuración y otras fuentes de datos para fines de depuración o resolución de problemas), verifique que el PAN quede ilegible de acuerdo con los requisitos del 2.3.a al 2.3.d, especificados arriba.</p>				

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>2.4 Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Las claves de descifrado no deben estar vinculadas a cuentas de usuarios.</p> <p>Concuerda con el Requisito 3.4.2 de las PCI DSS</p>	<p>2.4 Si se utiliza el cifrado de disco, compruebe que se implemente de la siguiente manera:</p> <p>2.4.a Verifique que el acceso lógico a los sistemas de archivos cifrados se implemente por medio de un mecanismo separado del mecanismo de los sistemas operativos nativos (por ejemplo, sin utilizar bases de datos de cuentas de usuarios locales).</p> <p>2.4.b Verifique que las claves criptográficas estén almacenadas de forma segura (por ejemplo, se almacenen en medios portátiles protegidos adecuadamente con controles sólidos de acceso).</p> <p>2.4.c Si la aplicación crea o genera archivos en medios removibles, verifique que los datos de los titulares de tarjeta que están en los medios removibles queden cifrados dondequiera que se almacenen.</p>			
<p>2.5 La aplicación de pago debe proteger las claves utilizadas para asegurar los datos de los titulares de tarjeta contra divulgación o uso indebido.</p> <p>Nota: Este requisito también se aplica a las claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos; tales claves de cifrado de claves deben ser por lo menos tan sólidas como la clave de cifrado de datos.</p> <p>Concuerda con el Requisito 3.5 de las PCI DSS</p>	<p>2.5 Verifique que la aplicación de pago proteja las claves utilizadas para asegurar los datos de titulares de tarjeta contra divulgación o uso indebido, de la siguiente manera:</p> <p>2.5.a Examine la metodología utilizada por la aplicación para proteger las claves, para comprobar que existen controles que restringen el acceso a las claves.</p> <p>2.5.b Examine los archivos de configuración del sistema para verificar que las claves se almacenan en formato cifrado y que las claves de cifrado de claves se almacenan separadas de la claves de cifrado de datos.</p> <p>2.5.c Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que los clientes y los revendedores/integradores reciban la recomendación de:</p> <ul style="list-style-type: none"> ▪ Restrinja el acceso a las claves al número mínimo de custodios necesarios. ▪ Guarde las claves de forma segura en la menor cantidad de ubicaciones y formas posibles. 			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>2.6 La aplicación de pago debe implementar los procesos y los procedimientos de gestión de claves respecto de las que se utilizan para el cifrado de datos de titulares de tarjetas, incluidos por lo menos los siguientes:</p> <p>Concuerda con el Requisito 3.6 de las PCI DSS</p>	<p>2.6.a Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores:</p> <ul style="list-style-type: none"> ▪ Cómo generar, distribuir, proteger, cambiar, almacenar y retirar/reemplazar claves de cifrado, cuando los clientes o revendedores/integradores participen en estas actividades de gestión de claves. ▪ Un formulario de Custodio de claves para que los custodios de las claves reconozcan que entienden y aceptan sus responsabilidades. ▪ Cómo realizar las funciones de gestión de claves que se definen abajo en 2.6.1 hasta 2.6.7, según se requiera para cumplir con las PCI DSS. <p>2.6.b Verifique que la aplicación de pago implemente técnicas de gestión de claves para las claves, de la siguiente manera:</p>			
<p>2.6.1 Generación de claves criptográficas sólidas</p>	<p>2.6.1 Verifique que los procedimientos de gestión de claves se hayan implementado para generar claves sólidas.</p>			
<p>2.6.2 Distribución segura de claves criptográficas</p>	<p>2.6.2 Verifique que los procedimientos de gestión de claves se hayan implementado para distribuir las claves de forma segura.</p>			
<p>2.6.3 Almacenamiento seguro de claves criptográficas</p>	<p>2.6.3 Verifique que los procedimientos de gestión de claves se hayan implementado para almacenar las claves de forma segura.</p>			
<p>2.6.4 La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria (por ejemplo, NIST Special Publication 800-57).</p>	<p>2.6.4 Verifique que los procedimientos de gestión de claves se hayan implementado para aplicar los cambios de clave al final del período de cifrado definido.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>2.6.5 Retiro o reemplazo de claves (por ejemplo: mediante archivo, destrucción y/o revocación según corresponda) según se considere necesario cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro, etc.) o se sospeche de que las claves están en riesgo.</p> <p><i>Nota: Si es necesario retener las claves criptográficas retiradas o reemplazadas, éstas se deben archivar de forma segura (por ejemplo, utilizando una clave de cifrado de claves). Las claves criptográficas archivadas se deben utilizar sólo con fines de descifrado/verificación.</i></p>	<p>2.6.5.a Verifique que los procedimientos de gestión de claves se hayan implementado para retirar las claves cuando se haya debilitado la integridad de las mismas.</p>			
	<p>2.6.5.b Verifique que los procedimientos de administración de clave se hayan implementado para reemplazar claves que se sepa o se sospeche que están en riesgo.</p>			
	<p>2.6.5.c Si se retienen las claves criptográficas retiradas o reemplazadas, verifique que la aplicación no las utilice para operaciones de cifrado.</p>			
<p>2.6.6 Si la aplicación de pago admite operaciones manuales de gestión de claves cartográficas en texto claro, estas operaciones deben aplicar conocimiento dividido y control doble (por ejemplo, utilizando dos o tres personas, cada una de las cuales conoce su propia parte de la clave, para reconstruir toda la clave).</p> <p><i>Nota: Los ejemplos de operaciones manuales de gestión de claves incluyen, entre otros: generación, transmisión, carga, almacenamiento y destrucción de claves.</i></p>	<p>2.6.6 Verifique que los procedimientos manuales de gestión de claves en texto claro requieran conocimiento dividido y control doble de las claves.</p>			
<p>2.6.7 Prevención de sustitución no autorizada de claves criptográficas</p>	<p>2.6.7 Verifique que los procedimientos de gestión de claves se hayan implementado para prevenir la sustitución no autorizada de claves.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>2.7 Haga que no se pueda recuperar ningún material de clave criptográfica o criptograma almacenado por las versiones anteriores de la aplicación de pago, de acuerdo con las normas aceptadas en la industria. Estas son las claves criptográficas que se utilizan para cifrar o verificar los datos de titulares de tarjetas.</p> <p>Notas:</p> <ul style="list-style-type: none"> ▪ <i>La recuperación de materiales de claves criptográficas y/o criptogramas se puede impedir utilizando herramientas o procesos que incluyen, entre otros:</i> <ul style="list-style-type: none"> – <i>Eliminación segura, según se define, por ejemplo, en la lista de productos aprobados que mantiene la Agencia de Seguridad Nacional u otra norma o reglamentación estatal o nacional.</i> – <i>La eliminación de la clave de cifrado de claves (KEK) siempre y cuando las claves de cifrado de datos residuales sólo existan en forma cifrada bajo la KEK eliminada.</i> ▪ <i>Este requisito sólo se aplica si hay versiones anteriores de la aplicación de pago que hayan utilizado materiales de claves criptográficas o criptogramas para cifrar datos de titulares de tarjetas.</i> <p>Concuerda con el Requisito 3.6 de las PCI DSS</p>	<p>2.7.a Revise la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores:</p> <ul style="list-style-type: none"> ▪ Que el material criptográfico debe quedar irrecuperable. ▪ Cómo impedir que el material criptográfico pueda ser recuperado. ▪ Que dicha incapacidad para recuperar el material es absolutamente necesaria para cumplir con las PCI DSS. ▪ Cómo volver a cifrar datos históricos con claves nuevas. <p>2.7.b Verifique que el proveedor proporcione una herramienta o un procedimiento para hacer que el material criptográfico sea irrecuperable.</p> <p>2.7.c Verifique, mediante el uso de herramientas y/o métodos forenses, que la herramienta o el procedimiento de limpieza segura haga que el material criptográfico sea irrecuperable, de acuerdo con las normas aceptadas en la industria.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
3. Proporcione funciones de autenticación segura				
<p>3.1 La aplicación de pago debe admitir y aplicar el uso de ID de usuario únicas y autenticación segura para todo acceso administrativo y para todo acceso a los datos de titulares de tarjeta. La autenticación segura se debe aplicar para todas las cuentas, generadas o administradas por la aplicación, al concluir la instalación y para cambios subsiguientes después de la instalación. La aplicación debe requerir lo siguiente:</p> <p><i>Nota: Estos controles de contraseña no se aplican a empleados que únicamente tienen acceso a un solo número de tarjeta a la vez para facilitar una transacción individual. Estos controles se pueden aplicar al acceso por parte de personal con funciones administrativas, al acceso a sistemas con datos de titulares de tarjeta y al acceso controlado por la aplicación de pago.</i></p> <p><i>Este requisito se debe implementar en la aplicación de pago y en todas las herramientas relacionadas que se utilizan para ver o acceder a los datos de titulares de tarjetas.</i></p> <p>Concuerda con los Requisitos 8.1, 8.2, y 8.5.8–8.5.15 de las PCI DSS</p>	<p>3.1.a Examine la <i>Guía de implementación de las PA-DSS</i> creada por el proveedor para verificar lo siguiente:</p> <ul style="list-style-type: none"> ▪ Se informa a los clientes y revendedores/integradores que la aplicación de pago aplica autenticación segura para todas las credenciales de autenticación que genera la aplicación al: <ul style="list-style-type: none"> – Aplicar los cambios seguros a las credenciales de autenticación una vez que finaliza la instalación (ver 3.1.1 hasta 3.1.10 abajo). – Aplicar los cambios seguros para cualquier cambio subsiguiente (después de la instalación) a las credenciales de autenticación (ver 3.1.1 hasta 3.1.10 abajo) ▪ Se informa a los clientes y revendedores/integradores que deben asignar autenticación segura a cualquier cuenta predeterminada (aun cuando no se utilicen) y, luego, desactivar las cuentas o no utilizarlas. ▪ Cuando la aplicación de pago utilice credenciales de autenticación (pero no las genere ni las administre), se proporcionarán a los clientes y revendedores/integradores instrucciones claras y precisas sobre cómo cambiar credenciales de autenticación o crear autenticación sólida, al concluir la instalación y para cambios después de la instalación, de acuerdo con los requisitos 3.1.1 hasta 3.1.10, que se describen abajo, para todas las cuentas a nivel de aplicación con acceso administrativo y para todo acceso a datos de titulares de tarjeta. <p>3.1.b Pruebe la aplicación de pago para verificar que se no utilicen (o se requiera el uso de) cuentas administrativas predeterminadas para otro software necesario (por ejemplo, la aplicación de pago no debe utilizar la cuenta administrativa predeterminada para el software de base de datos).</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
	<p>3.1.c Si la aplicación de pago genera o gestiona credenciales de autenticación, pruebe la aplicación para verificar que implementa los cambios a las contraseñas predeterminadas de la aplicación de pago al concluir del proceso de instalación.</p>			
	<p>3.1.d Para las cuentas que sean generadas o gestionadas por la aplicación, pruebe la aplicación para verificar que implementa las ID de usuario únicas y la autenticación segura de acuerdo con 3.1.1 hasta 3.1.10, que se describen abajo, para todo acceso administrativo y para todo acceso a los datos de los titulares de tarjeta.</p> <p>Asegúrese de que se apliquen los requisitos de autenticación segura:</p> <ul style="list-style-type: none"> - Al concluir el proceso de instalación, y - Para cambios subsiguientes después de la instalación. <p>(Los ejemplos de cambios subsiguientes incluyen, entre otros, cualquier cambio que ocasione que las cuentas de usuario regresen a la configuración predeterminada, cualquier cambio en la configuración actual de las cuentas y cambios que generen nuevas cuentas o vuelvan a crear cuentas ya existentes).</p>			
<p>3.1.1 La aplicación de pago asigna las ID únicas para las cuentas de usuario.</p> <p><i>Concuerda con el Requisito 8.1 de las PCI DSS</i></p>	<p>3.1.1 Confirme que la aplicación de pago asigne las ID de usuario únicas:</p>			
	<p>3.1.1.a Al concluir el proceso de instalación.</p>			
	<p>3.1.1.b Para cambios subsiguientes después de la instalación.</p>			
<p>3.1.2 La aplicación de pago emplea por lo menos uno de los siguientes métodos para autenticar a todos los usuarios:</p> <ul style="list-style-type: none"> ▪ Algo que el usuario sepa, como una contraseña o frase de seguridad ▪ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente ▪ Algo que el usuario sea, como un rasgo biométrico 	<p>3.1.2 Confirme que la aplicación de pago requiera por lo menos uno de los métodos de autenticación definidos:</p>			
	<p>3.1.2.a Al concluir el proceso de instalación.</p>			
	<p>3.1.2.b Para cambios subsiguientes después de la instalación.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
Concuerda con los Requisitos 8.2 de las PCI DSS				
3.1.3 La aplicación de pago no requiere ni utiliza cuentas y contraseñas de grupo, compartidas o genéricas.	3.1.3 Confirme que la aplicación de pago no dependa de, ni utilice, cuentas o contraseñas de grupo, compartidas o genéricas:			
Concuerda con el Requisito 8.5.8 de las PCI DSS	3.1.3.a Al concluir el proceso de instalación			
	3.1.3.b Para cambios subsiguientes después de la instalación.			
3.1.4 La aplicación de pago requiere que se cambien las contraseñas de usuario por lo menos cada 90 días.	3.1.4 Confirme que la aplicación de pago le solicita a los usuarios que cambien las contraseñas por lo menos cada 90 días:			
Concuerda con el Requisito 8.5.9 de las PCI DSS	3.1.4.a Al concluir el proceso de instalación			
	3.1.4.b Para cambios subsiguientes después de la instalación			
3.1.5 La aplicación de pago requiere una longitud de contraseña mínima de siete caracteres.	3.1.5 Confirme que la aplicación de pago requiere que las contraseñas tengan por lo menos siete caracteres:			
Concuerda con el Requisito 8.5.10 de las PCI DSS	3.1.5.a Al concluir el proceso de instalación			
	3.1.5.b Para cambios subsiguientes después de la instalación			
3.1.6 La aplicación de pago requiere que las contraseñas contengan caracteres numéricos y alfabéticos.	3.1.6 Confirme que la aplicación de pago requiera contraseñas que contengan caracteres numéricos y alfabéticos.			
Concuerda con el Requisito 8.5.11 de las PCI DSS	3.1.6.a Al concluir el proceso de instalación			
	3.1.6.b Para cambios subsiguientes después de la instalación			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>3.1.7 La aplicación de pago mantiene un historial de contraseñas y requiere que una contraseña nueva sea diferente de las cuatro últimas contraseñas utilizadas.</p> <p>Concuerda con el Requisito 8.5.12 de las PCI DSS</p>	<p>3.1.7 Confirme que la aplicación de pago mantenga un historial de contraseñas y requiera que una nueva contraseña sea diferente, por lo menos, de las últimas cuatro contraseñas utilizadas:</p>			
	<p>3.1.7.a Al concluir el proceso de instalación</p>			
	<p>3.1.7.b Para cambios subsiguientes después de la instalación</p>			
<p>3.1.8 La aplicación de pago limita los intentos de acceso repetidos bloqueando la cuenta del usuario después de más de seis intentos de inicio de sesión.</p> <p>Concuerda con el Requisito 8.5.13 de las PCI DSS</p>	<p>3.1.8 Confirme que la aplicación de pago bloquea las cuentas de usuario después de más de seis intentos de inicio de sesión no válidos.</p>			
	<p>3.1.8.a Al concluir el proceso de instalación</p>			
	<p>3.1.8.b Para cambios subsiguientes después de la instalación</p>			
<p>3.1.9 La aplicación de pago establece la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID de usuario.</p> <p>Concuerda con el Requisito 8.5.14 de las PCI DSS</p>	<p>3.1.9 Confirme que la aplicación de pago bloquee las cuentas de usuario por un mínimo de 30 minutos o hasta que un administrador del sistema restablezca la cuenta.</p>			
	<p>3.1.9.a Al concluir el proceso de instalación</p>			
	<p>3.1.9.b Para cambios subsiguientes después de la instalación</p>			
<p>3.1.10 Si una sesión de la aplicación de pago ha estado inactiva más de 15 minutos, la aplicación requiere una nueva autenticación del usuario para reactivar la sesión.</p> <p>Concuerda con el Requisito 8.5.15 de las PCI DSS</p>	<p>3.1.10 Confirme que la aplicación de pago establezca en 15 minutos o menos el tiempo de inactividad para bloquear una sesión.</p>			
	<p>3.1.10.a Al concluir el proceso de instalación</p>			
	<p>3.1.10.b Para cambios subsiguientes después de la instalación</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>3.2 El proveedor del software debe indicar a los clientes que todo acceso a computadoras, servidores y bases de datos con aplicaciones de pago debe requerir una ID de usuario única y autenticación segura.</p> <p>Concuerta con los Requisitos 8.1 y 8.2 de las PCI DSS</p>	<p>3.2 Examine la <i>Guía de implementación de las PA-DSS</i> creada por el proveedor para verificar que se les sugiera firmemente a los clientes y revendedores/integradores que controlen el acceso a cualquier computadora, servidor y base de datos que tenga aplicaciones de pago y datos de titulares de tarjetas por medio de una ID de usuario única y una autenticación segura que cumpla con las PCI DSS.</p>			
<p>3.3 Haga que las contraseñas de la aplicación de pago sean ilegibles durante la transmisión y el almacenamiento, usando criptografía sólida basada en las normas aprobadas.</p> <p>Concuerta con el Requisito 8.4 de las PCI DSS</p>	<p>3.3 Examine los archivos de contraseña de la aplicación de pago durante el almacenamiento y la transmisión a fin de verificar que se utiliza criptografía sólida para impedir en todo momento que las contraseñas puedan ser leídas.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
4. Registre la actividad de la aplicación de pago				
<p>4.1 Al concluir el proceso de instalación, la instalación simple predeterminada de la aplicación de pago debe registrar todos los accesos de los usuarios (en especial de los que tienen privilegios administrativos), y debe poder vincular todas las actividades con usuarios individuales.</p> <p>Concuerda con Requisito 10.1 de las PCI DSS</p>	<p>4.1.a Examine los valores de configuración de la aplicación de pago para verificar que las pistas de auditoría se activen automáticamente o estén a disposición de los clientes para ser activadas.</p> <p>4.1.b Si los valores de configuración de registro de la aplicación de pago pueden ser definidos por el cliente y los revendedores/integradores, o si los clientes o revendedores/integradores son responsables de implementar el registro, examine la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor para verificar que se incluya la siguiente información:</p> <ul style="list-style-type: none"> ▪ Cómo establecer los valores de configuración del registro para que cumplan con las PCI DSS, según los requisitos 4.2, 4.3 y 4.4 de las PA-DSS que se describen abajo. ▪ Que no se desactiven los registros, ya que al hacerlo se incumpliría con las PCI DSS. 			
<p>4.2 La aplicación de pago debe proporcionar una pista de auditoría para reconstruir los siguientes eventos:</p> <p>Concuerda con el Requisito 10.2 de las PCI DSS</p>	<p>4.2 Pruebe la aplicación de pago y examine los registros de auditoría y la configuración de los registros de auditoría de la aplicación de pago, y haga lo siguiente:</p>			
<p>4.2.1 Todos los accesos individuales a los datos de titulares de tarjeta desde la aplicación</p>	<p>4.2.1 Verifique que se registra todo acceso individual a datos de titulares de tarjeta a través de la aplicación de pago.</p>			
<p>4.2.2 Todas las acciones realizadas por un individuo con privilegios administrativos asignados en la aplicación</p>	<p>4.2.2 Verifique que se registren todas las acciones realizadas por un individuo con privilegios administrativos para la aplicación de pago.</p>			
<p>4.2.3 Acceso a las pistas de auditoría de la aplicación que sean administradas por la aplicación o estén dentro de ella.</p>	<p>4.2.3 Verifique que se registre el acceso a las pistas de auditoría de la aplicación que sean administradas por la aplicación o estén dentro de ella .</p>			
<p>4.2.4 Intentos de acceso lógico no válidos</p>	<p>4.2.4 Verifique que se registren los intentos de acceso lógico no válidos.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
4.2.5 Uso de los mecanismos de identificación y autenticación de la aplicación	4.2.5 Verifique que se registre el uso de los mecanismos de identificación y autenticación de la aplicación.			
4.2.6 Inicialización de los registros de auditoría de la aplicación	4.2.6 Verifique que se registre la inicialización de los registros de auditoría de la aplicación.			
4.2.7 Creación y eliminación de objetos a nivel de sistema dentro de la aplicación o por la aplicación	4.2.7 Verifique se registre la creación y eliminación de objetos a nivel de sistema dentro de la aplicación o por la aplicación.			
4.3 La aplicación de pago debe registrar por lo menos las siguientes entradas de la pista de auditoría para cada evento: Concuerda con el Requisito 10.3 de las PCI DSS	4.3 Pruebe la aplicación de pago y examine los registros de auditoría de la aplicación y la configuración de los registros de auditoría y, para cada evento auditable (según 4.2), realice lo siguiente:			
4.3.1 Identificación de usuarios	4.3.1 Verifique que la identificación de usuarios se incluya en las entradas del registro.			
4.3.2 Tipo de evento	4.3.2 Verifique que el tipo de evento se incluya en las entradas del registro.			
4.3.3 Fecha y hora	4.3.3 Verifique que el sello de fecha y hora se incluya en las entradas del registro.			
4.3.4 Indicación de éxito o fallo	4.3.4 Verifique que la indicación de éxito o fallo se incluya en las entradas del registro.			
4.3.5 Origen del evento	4.3.5 Verifique que el origen del evento se incluya en las entradas del registro.			
4.3.6 Identidad o nombre de los datos, componentes del sistema o recurso afectados	4.3.6 Verifique que la identidad o nombre de los datos, componentes del sistema o recursos afectados se incluya en las entradas del registro.			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>4.4. La aplicación de pago debe facilitar el registro centralizado.</p> <p>Nota: Los ejemplos de esta funcionalidad pueden incluir, entre otros:</p> <ul style="list-style-type: none"> ▪ Realizar registros utilizando mecanismos de archivos de registro estándar en la industria, como el Sistema de Archivos de Registro Comunes (CLFS), Syslog, texto delimitado, etc. ▪ Proporcionar funciones y documentación para convertir el formato de registro patentado de la aplicación en formatos de registro estándar en la industria adecuados para un registro inmediato y centralizado. <p>Concuerda con el Requisito 10.5.3 de las PCI DSS</p>	<p>4.4.a Confirme que la aplicación de pago proporciona funciones que facilitan la capacidad del comerciante para integrar los registros a su servidor centralizado de registros.</p>			
	<p>4.4.b Examine la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor para verificar que a los clientes y los revendedores/integradores se les proporcionan instrucciones y procedimientos para incorporar los registros de la aplicación de pago a su entorno de registro centralizado.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
5. Desarrolle aplicaciones de pago seguras				
<p>5.1 El proveedor del software desarrolla las aplicaciones de pago conforme a las PCI DSS y las PA-DSS (por ejemplo, registro y autenticación seguros) sobre la base de las mejores prácticas de la industria, e incorpora la seguridad de la información en todo el ciclo de desarrollo de software. Estos procesos deben incluir lo siguiente:</p> <p>Concuerda con el Requisito 6.3 de las PCI DSS</p>	<p>5.1.a Obtenga y examine los procesos de desarrollo de software escritos para verificar que los procesos estén basados en normas de la industria y/o en las mejores prácticas.</p> <p>5.1.b Verifique que se incluya la seguridad de la información en todo el ciclo de desarrollo de software.</p> <p>5.1.c Verifique que las aplicaciones de software se desarrollen de acuerdo con los requisitos de las PCI DSS y las PA-DSS.</p> <p>5.1.d Utilizando una evaluación de los procesos de desarrollo de software escritos, entrevistas a los desarrolladores de software y una evaluación del producto final de aplicación de pago, verifique que:</p>			
<p>5.1.1 Los PAN activos no se utilizan para las pruebas ni para el desarrollo.</p> <p>Concuerda con el Requisito 6.4.3 de las PCI DSS</p>	<p>5.1.1 Los PAN activos no se utilizan para las pruebas ni para el desarrollo.</p>			
<p>5.1.2 Retiro de los datos y cuentas de prueba antes de entregar el producto al cliente.</p> <p>Concuerda con el Requisito 6.4.4 de las PCI DSS</p>	<p>5.1. 2 Los datos y las cuentas de prueba son retirados antes de entregar el producto al cliente.</p>			
<p>5.1.3 Retiro de las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago antes de que se les envíen a los clientes las aplicaciones de pago</p> <p>Concuerda con el Requisito 6.3.1 de las PCI DSS</p>	<p>5.1.3 Las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago son retiradas antes de entregar la aplicación de pago a los clientes.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>5.1.4 Revisión del código de la aplicación de pago antes del envío a los clientes después de algún cambio significativo, a fin de identificar la potencial vulnerabilidad de la codificación.</p> <p><i>Nota: Este requisito de revisiones de códigos se aplica a todos los componentes de la aplicación de pago (tanto las aplicaciones internas como las aplicaciones web disponibles para el público), como parte del ciclo de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento.</i></p> <p>Concuerda con el Requisito 6.3.2 de las PCI DSS</p>	<p>5.1.4 Confirme que el proveedor realiza revisiones de los códigos para todo los cambios significativos en los códigos de la aplicación (utilizando procesos manuales o automatizados), de la manera siguiente:</p> <ul style="list-style-type: none"> ▪ Los cambios a los códigos son revisados por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura. ▪ Las revisiones de los códigos se desarrollan de acuerdo con las directrices de codificación segura. (Consulte el Requisito 5.2. de las PA-DSS) ▪ Las correcciones pertinentes se implementan antes del lanzamiento. ▪ La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. 			
<p>5.2 Desarrolle todas las aplicaciones de pago (internas y externas, que incluyan acceso administrativo web al producto) basándose en las directrices de codificación segura. Considere la prevención de las vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir:</p> <p><i>Nota: Las vulnerabilidades indicadas en los requisitos 5.2.1 hasta 5.2.9 de las PA-DSS y 6.5.1 hasta 6.5.9 de las PCI DSS eran congruentes con las mejores prácticas de la industria cuando se publicó esta versión de las PA DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.</i></p> <p>Concuerda con el Requisito 6.5 de las PCI DSS</p>	<p>5.2.a Obtenga y revise los procesos de desarrollo de software relacionados con las aplicaciones de pago (internas y externas, con inclusión de acceso administrativo web al producto). Compruebe que el proceso incluya capacitación acerca de las técnicas de codificación segura para desarrolladores, que esté basada en las mejores prácticas de la industria, así como asesoría.</p>			
	<p>5.2.b Entreviste a un grupo modelo de desarrolladores y obtenga pruebas de que son expertos en técnicas de codificación segura.</p>			
	<p>5.2.c Verifique que las aplicaciones de pago no sean susceptibles a las vulnerabilidades de codificación comunes realizando pruebas de penetración manuales o automatizadas que intenten explotar específicamente cada uno de los siguientes errores:</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
5.2.1 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.	5.2.1 Errores de inyección, en especial, errores de inyección SQL (valide la entrada para verificar que los datos de usuario no pueden modificar el significado de los comandos y las consultas, utilice las consultas basadas en parámetros, etc.).			
5.2.2 Desbordamiento de buffer	5.2.2 Desbordamiento de buffer (validar límites del buffer y truncar cadenas de entrada).			
5.2.3 Almacenamiento criptográfico inseguro	5.2.3 Almacenamiento criptográfico inseguro (prevenir defectos de criptografía).			
5.2.4 Comunicaciones inseguras	5.2.10 Comunicaciones inseguras (cifrar adecuadamente todas las comunicaciones autenticadas y confidenciales).			
5.2.5 Manejo inadecuado de errores	5.2.5 Manejo inadecuado de errores (no permitir que se filtre información a través de mensajes de error)			
5.2.6 Todas las vulnerabilidades “altas” detectadas en el proceso de identificación de vulnerabilidades en el Requisito 7.1 de las PA-DSS	5.2.6 Todas las vulnerabilidades “altas” identificadas en el Requisito 7.1 de las PA-DSS			
Nota: Los requisitos del 5.2.7 al 5.2.9, que siguen, se aplican a las aplicaciones basadas en la web y a las interfaces de aplicaciones (internas o externas):				
5.2.7 Lenguaje de comandos entre distintos sitios (XSS)	5.2.7 Lenguaje de comandos entre distinto sitios (XSS) (valide todos los parámetros antes de la inclusión, utilice técnicas de escape sensibles al contexto, etc.)			
5.2.8 Control de acceso inapropiado tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios)	5.2.8 Referencias no seguras a objetos directos (Autentique usuarios de forma correcta y desinfecte entradas. No exponga referencias a objetos internos a usuarios).			
5.2.9 Falsificación de solicitudes entre distintos sitios (CSRF)	5.2.9 Falsificación de solicitudes entre distintos sitios (CSRF) (no confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente).			
5.3 El proveedor de software debe seguir los procedimientos de control de cambios para todos los cambios que surjan en la configuración del software de productos. Los procedimientos deben	5.3.a Obtenga y examine los procedimientos de control de cambios del proveedor para las modificaciones del software y verifique que los procedimientos exijan los puntos del 5.3.1 al 5.3.4, que aparecen a continuación.			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
incluir lo siguiente: Concuerda con el requisito 6.4.5 de las PCI DSS	5.3.b Examine los cambios recientes en la aplicación de pago y realice un seguimiento de los cambios relacionados con la documentación de control de cambios. Verifique que, para cada cambio examinado, se haya documentado lo siguiente de acuerdo con los procedimientos de control de cambios:			
5.3.1 Documentación de incidencia	5.3.1 Verifique que la documentación que tiene incidencia en el cliente se incluya en la documentación de control de cambios de cada cambio.			
5.3.2 Aprobación de cambio documentada por las partes autorizadas apropiadas	5.3.2 Verifique que la aprobación documentada por las partes autorizadas apropiadas esté presente para cada cambio.			
5.3.3 Verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.	5.3.3.a Para cada cambio probado, verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema			
	5.3.3.b Verifique que todos los cambios (incluidos los parches) se hayan sometido a prueba a fin de determinar si cumplen con el punto 5.2 antes del lanzamiento.			
5.3.4 Procedimientos de detención o desinstalación del producto	5.3.4 Verifique que los procedimientos de detención o desinstalación del producto estén preparados para cada cambio.			
5.4 La aplicación de pago sólo debe utilizar o requerir el uso de servicios, protocolos, daemons, componentes, así como software y hardware dependientes, necesarios y seguros, incluidos los proporcionados por terceros, para cualquier funcionalidad de la aplicación de pago (por ejemplo, si la aplicación requiere NetBIOS, archivos compartidos, Telnet, FTP, etc., éstos se aseguran a través de SSH, S-FTP, SSL, IPsec u otra tecnología). Concuerda con el requisito 2.2.2 de las PCI DSS	5.4.a Examine los servicios, protocolos, daemons, componentes y software y hardware dependientes del sistema activados o requeridos por la aplicación de pago. Verifique que sólo los servicios, protocolos, daemons, componentes, software y hardware dependientes necesarios y seguros se encuentren activados por opción predeterminada			
	5.4.b Si la aplicación admite servicios, daemons, protocolos o componentes no seguros, verifique que se encuentren configurados de forma segura por opción predeterminada.			
	5.4.c Verifique que la <i>Guía de implementación de las PA-DSS</i> documente todos los protocolos, servicios, componentes, y software y hardware dependientes requeridos que son necesarios para cualquier funcionalidad de la aplicación de pago, incluidos los proporcionados por terceros.			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
6. Proteja las transmisiones inalámbricas				
<p>6.1 Para las aplicaciones de pago que utilizan tecnología inalámbrica, cambie los valores predeterminados inalámbricos proporcionados por los proveedores, incluidos, a título enunciativo y no taxativo, claves de cifrado para conexiones inalámbricas, contraseñas y cadenas de comunidad SNMP. La tecnología inalámbrica se debe implementar de forma segura.</p> <p>Concuerda con los requisitos 1.2.3 y 2.1.1 de las PCI DSS</p>	<p>6.1 En cuanto a las aplicaciones de pago desarrolladas por el proveedor con tecnología inalámbrica y otras aplicaciones inalámbricas combinadas con la aplicación de pago, verifique que las aplicaciones inalámbricas no utilicen los valores de configuración predeterminados por el proveedor, de la siguiente manera:</p>			
	<p>6.1.a Verifique que las claves de cifrado predeterminadas se hayan cambiado al momento de la instalación y que se cambien cada vez que una persona con conocimiento de éstas cese en sus funciones o se traslade a otro cargo en la empresa</p>			
	<p>6.1.b Verifique que se hayan cambiado las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos</p>			
	<p>6.1.c Verifique que se hayan cambiado las contraseñas predeterminadas de los puntos de acceso</p>			
	<p>6.1.d Verifique que el firmware de los dispositivos inalámbricos esté actualizado a los efectos de admitir el cifrado sólido para la autenticación y transmisión en redes inalámbricas</p>			
	<p>6.1.e Verifique que se hayan cambiado otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
	<p>6.1.f Consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor para verificar que los clientes y los revendedores/integradores reciban instrucciones, cuando se utilice la modalidad inalámbrica, para:</p> <ul style="list-style-type: none"> ▪ Cambiar los valores predeterminados proporcionados por el proveedor relacionados con la modalidad inalámbrica, según se definió anteriormente en 6.1.a a 6.1.e; ▪ Instalar un firewall entre las redes inalámbricas y los sistemas que almacenen datos del titular de la tarjeta, y ▪ Configurar los firewalls para negar o controlar (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde cualquier entorno inalámbrico hacia el entorno de datos del titular de la tarjeta. 			
<p>6.2 Con el fin de simplificar la utilización de las mejores prácticas de la industria (por ejemplo, IEEE 802.11i), las aplicaciones de pago que utilizan tecnología inalámbrica deben implementar un cifrado sólido para la autenticación y transmisión.</p> <p>Nota: La utilización de WEP como control de seguridad se prohibió a partir del 30 de junio de 2010.</p> <p>Concuerda con el requisito 4.1.1 de las PCI DSS</p>	<p>6.2.a En cuanto a las aplicaciones de pago desarrolladas por el proveedor con tecnología inalámbrica y otras aplicaciones inalámbricas combinadas con la aplicación del proveedor, verifique que se hayan utilizado las mejores prácticas de la industria (por ejemplo, IEEE 802.11.i) con la finalidad de incluir o poner a disposición un cifrado sólido para la autenticación y transmisión.</p> <p>6.2.b Si los clientes pueden implementar la aplicación de pago en un entorno inalámbrico, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor para verificar que los clientes y revendedores/integradores reciban instrucciones sobre la configuración inalámbrica que cumple con las PCI DSS, incluidos el cambio de los valores predeterminados proporcionados por los proveedores (según 6.1.a – 6.1.e, especificados anteriormente) y el uso de las mejores prácticas de la industria para implementar un cifrado sólido para la autenticación y transmisión de los datos del titular de la tarjeta (según 6.2.a).</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
7. Pruebe las aplicaciones de pago para tratar las vulnerabilidades				
<p>7.1 Los proveedores de software deben establecer un proceso para identificar y asignar una clasificación de riesgo a las vulnerabilidades de seguridad recientemente descubiertas y para probar sus aplicaciones a fin de determinar la presencia de vulnerabilidades. En este proceso, se debe incluir todo software o sistema subyacente que provea o requiera la aplicación de pago (por ejemplo, los servidores web, programas y bibliotecas de terceros).</p> <p>Concuerda con el Requisito 6.2 de las PCI DSS</p> <p>Nota: Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria. Por ejemplo, los criterios para clasificar vulnerabilidades de "Alto" riesgo pueden incluir una puntuación base CVSS de 4.0 o superior, y/o un parche proporcionado por el proveedor clasificado por el mismo como "crítico", y/o una vulnerabilidad que afecte un componente crítico de la aplicación.</p>	<p>7.1 Obtenga y consulte los procesos para identificar nuevas vulnerabilidades y para probar aplicaciones de pago para determinar la presencia de nuevas vulnerabilidades. Verifique que los procesos incluyan lo siguiente:</p>			
	<p>7.1.a Verifique que los procesos incluyan la asignación de una clasificación de riesgo a las vulnerabilidades identificadas. (Como mínimo, las vulnerabilidades más críticas que representen los riesgos más altos se deben clasificar como "Alto".)</p>			
	<p>7.1.b Verifique que los procesos para identificar las nuevas vulnerabilidades de seguridad incluyan el uso de fuentes externas de información sobre vulnerabilidades de seguridad</p>			
	<p>7.1.c Verifique que los procesos incluyan la realización de pruebas a las aplicaciones de pago para determinar la presencia de nuevas vulnerabilidades</p>			
	<p>7.1.d Verifique que los procesos para identificar las nuevas vulnerabilidades e implementar correcciones en la aplicación de pago sean de aplicación en todo el software que provee o exige la aplicación de pago (por ejemplo, servidores web, programas y bibliotecas de terceros).</p>			
<p>7.2 Los proveedores de software deben establecer un proceso para el desarrollo y la implementación oportunos de parches y actualizaciones de seguridad, que incluya la entrega de actualizaciones y parches de manera segura con una conocida cadena de confianza, y el mantenimiento de la integridad del código de parche y actualización durante la entrega y la implementación.</p>	<p>7.2.a Obtenga y consulte procesos para desarrollar e implementar parches y actualizaciones de seguridad para software. Verifique que los procesos incluyan el desarrollo y la implementación oportunos de parches para los clientes</p>			
	<p>7.2.b Revise los procesos para verificar que los parches y las actualizaciones se distribuyan de manera segura a través de una cadena de confianza conocida</p>			
	<p>7.2.c Revise los procesos para verificar que los parches y las actualizaciones de distribuyan de manera que se preserve la integridad de los que se entrega</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
	7.2.d Revise los procesos para verificar que se haya probado la integridad de los parches y las actualizaciones en el sistema objetivo antes de la instalación			
	7.2.e Para verificar que se mantenga la integridad del código del parche y la actualización, ejecute el proceso de actualización con código arbitrario y determine si el sistema no permitirá que se lleve a cabo la actualización.			
8. Facilite la implementación de una red segura				
<p>8.1 La aplicación de pago debe ser capaz de implementarse en un entorno de red seguro. La aplicación no debe interferir con el uso de dispositivos, aplicaciones ni configuraciones que se requieran para cumplir con las PCI-DSS (por ejemplo, la aplicación de pago no puede interferir en la protección antivirus, las configuraciones de firewall ni ningún otro dispositivo, aplicación o configuración que se requiera para cumplir en las PCI-DSS).</p> <p>Concuerda con los Requisitos 1, 3, 4, 5 y 6 de las PCI DSS</p>	<p>8.1 Pruebe la aplicación de pago en un laboratorio para obtener pruebas de que se puede ejecutar en una red que cumple plenamente con lo establecido en las PCI DSS. Verifique que la aplicación de pago no inhiba la instalación de parches ni actualizaciones a otros componentes del entorno.</p>			
9. Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet				
<p>9.1 La aplicación de pago se debe desarrollar de manera que el servidor de base de datos y el servidor web no tengan que estar en el mismo servidor ni se requiera que el servidor de base de datos se encuentre en la DMZ del servidor web.</p> <p>Concuerda con el Requisito 1.3.7 de las PCI DSS</p>	<p>9.1.a A fin de verificar que la aplicación de pago almacena los datos de titulares de tarjetas en la red interna y nunca en la DMZ, obtenga evidencia de que la aplicación de pago no requiere el almacenamiento de datos en la DMZ y que permitirá el uso de una DMZ para separar Internet de los sistemas que almacenan datos de titulares de tarjetas (por ejemplo, la aplicación de pago no debe requerir que un servidor de base de datos y un servidor web se encuentren en el mismo servidor o en la DMZ con el servidor web).</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
	<p>9.1.b Si los clientes pudieran almacenar datos de titulares de tarjetas en un servidor conectado a Internet, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor para verificar si a los clientes y revendedores/integradores se les informó que no deben almacenar datos de titulares de tarjetas en sistemas a los que se pueda acceder desde Internet (por ejemplo, el servidor web y el servidor de la base de datos no deben estar en el mismo servidor).</p>			
<p>10. Facilite un acceso remoto seguro a la aplicación de pago.</p>				
<p>10.1 La aplicación de pago no debe interferir con el uso de tecnologías de autenticación de dos factores para el acceso remoto seguro. (Por ejemplo, RADIUS con tokens, TACACS con tokens u otras tecnologías que faciliten la autenticación de dos factores).</p> <p>Nota: La autenticación de dos factores requiere que dos de los tres métodos de autenticación (ver abajo) se utilicen para la autenticación. El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de dos factores. Los métodos de autenticación, también denominados factores, son:</p> <ul style="list-style-type: none"> ▪ Algo que el usuario sepa, como una contraseña o frase de seguridad ▪ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente ▪ Algo que el usuario sea, como un rasgo biométrico <p>Concuerda con el Requisito 8.3 de las PCI DSS</p>	<p>10.1 Pruebe la aplicación de pago en un laboratorio para obtener pruebas de que no interfiere con las tecnologías de autenticación de dos factores.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>10.2 Si se puede acceder a la aplicación de pago de manera remota, el acceso remoto debe ser autenticado mediante el uso de un mecanismo de autenticación de dos factores.</p> <p><i>Nota: La autenticación de dos factores requiere que dos de los tres métodos de autenticación se utilicen para la autenticación (consulte el requisito 10.1 de las PCI DSS para obtener una descripción de los métodos de autenticación).</i></p> <p>Concuerda con el Requisito 8.3 de las PCI DSS</p>	<p>10.2 Si se puede acceder a la aplicación de pago de manera remota, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor de software y verifique que contenga las instrucciones para los clientes y revendedores/integradores respecto del uso requerido de la autenticación de dos factores (dos de los tres métodos de autenticación descritos en el requisito 10.1 de las PA DSS).</p>			
<p>10.3 Cualquier acceso remoto a la aplicación de pago se debe realizar de forma segura, de la siguiente manera:</p>	<p>10.3 Verifique que cualquier acceso remoto se realice de la siguiente manera:</p>			
<p>10.3.1 Si las actualizaciones de la aplicación de pago se entregan mediante acceso remoto a los sistemas de los clientes, los proveedores de software deben informar a los clientes que enciendan las tecnologías de acceso remoto solamente cuando sea necesario para realizar descargas desde el proveedor y que lo apaguen inmediatamente después de finalizada la descarga.</p> <p>De manera alternativa, si se entregan por medio de VPN u otra conexión de alta velocidad, los proveedores de software deben sugerirles a sus clientes cómo configurar correctamente un firewall o un producto firewall personal a fin de asegurar conexiones “siempre activas”.</p> <p>Concuerda con los Requisitos 1 y 12.3.9 de las PCI DSS</p>	<p>10.1 Si el proveedor entrega la aplicación de pago y/o las actualizaciones por medio de un acceso remoto a las redes del cliente, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y verifique que contenga lo siguiente:</p> <ul style="list-style-type: none"> ▪ Las instrucciones para los clientes y revendedores/integradores respecto del uso seguro de tecnologías de acceso remoto, las cuales especifican que dichas tecnologías utilizadas por los proveedores y socios comerciales se deben activar sólo cuando sea necesario y desactivar inmediatamente después de utilizarlas. ▪ La recomendación para los clientes y los revendedores/integradores de que utilicen un firewall o un producto firewall personal en caso de que la computadora esté conectada por VPN u otra conexión de alta velocidad, a fin de asegurar estas conexiones "siempre activas" de conformidad con el requisito 1 de las PCI DDS. 			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>10.3.2 Si los proveedores, revendedores/integradores o clientes pueden acceder de manera remota a las aplicaciones de pago de los clientes, el acceso remoto se</p>	<p>10.3.2.a Si el proveedor de software utiliza productos de acceso remoto para acceder de manera remota a la aplicación de pago de los clientes, verifique que el personal del proveedor implemente y utilice las funciones de seguridad para acceso remoto.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>debe implementar de manera segura.</p> <p>Nota: Algunos ejemplos de funciones de seguridad para acceso remoto son:</p> <ul style="list-style-type: none"> ▪ Cambiar los valores de configuración predeterminados en el software de acceso remoto (por ejemplo, cambiar las contraseñas predeterminadas y utilizar contraseñas únicas para cada cliente). ▪ Permitir conexiones únicamente provenientes de direcciones IP/MAC (conocidas) específicas. ▪ Utilizar autenticación sólida y contraseñas complejas para inicios de sesión (Consulte los Requisitos 3.1.1 al 3.1.10 de las PA-DSS) ▪ Activar la transmisión de datos cifrados de acuerdo con el requisito 12.1 de las PCI DSS ▪ Activar el cierre de cuenta después de un determinado número de intentos fallidos de inicio de sesión (Consulte el Requisito 3.1.8 de las PA-DSS). ▪ Configurar el sistema de manera que un usuario remoto deba establecer una conexión de red privada virtual (VPN) mediante un firewall antes de que se le permita el acceso. ▪ Activar la función de inicio de sesión. ▪ Restringir el acceso a las contraseñas del cliente únicamente a personal autorizado del revendedor/integrador. ▪ Establecer contraseñas para clientes de acuerdo con los requisitos 3.1.1 al 3.1.10 de las PCI DSS. <p>Concuerda con el Requisito 8.3 de las PCI DSS</p>	<p>10.3.2.b Si los revendedores/integradores o clientes pueden utilizar un software de acceso remoto, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor de software y verifique que los clientes y revendedores/integradores hayan recibido instrucciones para utilizar e implementar funciones de seguridad para acceso remoto.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
11. Cifre el tráfico sensitivo de las redes públicas				
<p>11.1 Si la aplicación de pago envía o facilita el envío de datos de los tarjetahabientes por redes públicas, la aplicación de pago debe respaldar el uso de cifrado sólido o de protocolos de seguridad (por ejemplo, SSL/TLS, seguridad del protocolo Internet (IPSEC), SSH, etc.) para proteger datos sensitivos del titular de la tarjeta durante la transmisión por redes públicas abiertas.</p> <p><i>Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las DSS de la PCI son:</i></p> <ul style="list-style-type: none"> ▪ <i>The Internet</i> ▪ <i>Tecnologías inalámbricas</i> ▪ <i>Sistema global para comunicaciones móviles (GSM)</i> ▪ <i>Servicio de radio paquete general (GPRS)</i> <p>Concuerda con el Requisito 4.1 de las PCI DSS</p>	<p>11.1.a Si la aplicación de pago envía o facilita el envío de datos de los tarjetahabientes por redes públicas, verifique que se suministren tecnología de cifrado sólido o protocolos de seguridad o que se especifique el uso de éstos.</p> <p>11.1.b Si la aplicación de pago permite la transmisión de datos mediante redes públicas, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y verifique que se incluyan las directivas para los clientes y revendedores/integradores sobre cómo utilizar la tecnología de cifrado sólido y protocolos de seguridad.</p>			
<p>11.2 Si la aplicación de pago facilita el envío de PANs mediante las tecnologías de mensajería del usuario final (por ejemplo, correo electrónico, mensajería instantánea, chat), la aplicación de pago debe proporcionar una solución que haga que el PAN no sea legible o implemente un cifrado sólido o especificar el uso de cifrado sólido para cifrar los PANs.</p> <p>Concuerda con el Requisito 4.2 de las PCI DSS</p>	<p>11.2.a Si la aplicación de pago permite y/o facilita el envío de PAN por medio de tecnologías de mensajería de usuario final, verifique que se le provea una solución que haga el PAN no legible o que implemente un cifrado sólido, o bien que se le especifique cómo utilizarla.</p> <p>11.2.b Si la aplicación de pago permite y/o facilita el envío de PAN por medio de tecnologías de mensajería de usuario final, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe que se incluyan las directivas para los clientes y revendedores/integradores sobre cómo utilizar una solución de cifrado que haga el PAN no legible o que implemente un cifrado sólido.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
12. Cifre el acceso administrativo que no sea de consola				
<p>12.1 Instruya a los clientes para que cifren todo el acceso administrativo que no sea de consola con tecnologías de cifrado sólido como SSH, VPN o SSL/TLS para la administración basada en la web u otro acceso administrativo que no sea de consola.</p> <p><i>Nota: Nunca se deben utilizar Telnet ni rlogin para un acceso administrativo.</i></p> <p>Concuerda con el Requisito 2.3 de las PCI DSS</p>	<p>12.1 Si la aplicación de pago o el servidor permite la administración que no sea de consola, consulte la <i>Guía de implementación de las PA-DSS</i> preparada por el proveedor y compruebe si se recomienda el uso de cifrado sólido, tal como SSH, VPN o SSL/TLS para el cifrado del acceso administrativo que no sea de consola.</p>			
13. Mantenga la documentación instructiva y los programas de capacitación para clientes, revendedores e integradores				
<p>13.1 Desarrolle, mantenga y difunda una <i>Guía de implementación de las PA-DSS</i> para clientes, revendedores e integradores que cumpla con lo siguiente:</p>	<p>13.1.1 Consulte la <i>Guía de implementación de las PA-DSS</i> y procesos relacionados y verifique que la Guía sea distribuida a todos los usuarios de la aplicación de pago relevantes (incluyendo clientes, revendedores e integradores).</p>			
<p>13.1.1 Aborda todos los requisitos del presente documento siempre que se haga referencia a la <i>Guía de implementación de las PA-DSS</i>.</p>	<p>13.1.1 Verifique que la <i>Guía de implementación de las PA-DSS</i> considere todos los requisitos relacionados del presente documento.</p>			
<p>13.1.2.a Incluye por lo menos una revisión y actualización anual, para mantener la documentación actualizada de todos los cambios importantes y menores del software así como de los cambios a los requisitos de este documento.</p>	<p>13.1.2.a Verifique que la <i>Guía de implementación de las PA-DSS</i> se revise con una frecuencia anual y se actualice según sea necesario para documentar todos los cambios importantes y menores de la aplicación de pago.</p> <p>Verifique que la Guía de implementación de las PA-DSS se revise con una frecuencia anual y se actualice según sea necesario para documentar los cambios a los requisitos de las PA-DSS.</p>			

Requisitos de las PA-DSS	Procedimientos de prueba	Impleme ntado	No impleme ntado	Fecha objetivo y comentarios
<p>13.2 Desarrolle e implemente los programas de capacitación y comunicación para asegurar que los revendedores e integradores sepan cómo implementar la aplicación de pago y los sistemas y las redes afines de acuerdo con la Guía de implementación de las PA-DSS de conformidad con las PCI DSS.</p>	<p>13.2 Examine los materiales de capacitación y el programa de comunicación para revendedores e integradores y confirme si los materiales consideran todos los rubros analizados en la <i>Guía de implementación de las PA-DSS</i> en todo el documento.</p>			
<p>13.2.1 Actualice los materiales de capacitación anualmente y cada vez que se disponga de una nueva versión de la aplicación de pago.</p>	<p>13.2.1.a Examine los materiales de capacitación y el programa de comunicación para revendedores e integradores y verifique si los materiales son revisados anualmente y cuando se dispone de una nueva versión de la aplicación de pago y actualizados, según sea necesario.</p>			
	<p>13.2.1.b Examine el proceso de distribución para las nuevas versiones de la aplicación de pago y verifique que la documentación actualizada se distribuya junto con la aplicación de pago actualizada.</p>			
	<p>13.2.1.b Seleccione una muestra de revendedores e integradores y entrevístelos para comprobar que hayan recibido los materiales de capacitación.</p>			

Anexo A: Resumen de contenidos para la *Guía de implementación de las PA-DSS*

Este Anexo fue redactado con el propósito de resumir los requisitos de las PA-DSS que tienen temas relacionados con la *Guía de implementación de las PA-DSS*, a fin de explicar el contenido de la *Guía* y describir las responsabilidades de implementar los controles relacionados.

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
1.1.4	Borre los datos confidenciales de autenticación almacenados por las versiones anteriores de la aplicación de pago.	<ul style="list-style-type: none"> Se deben eliminar los datos históricos (datos de la banda magnética, códigos de verificación de la tarjeta, PIN o bloqueos de PIN almacenados por versiones anteriores de la aplicación de pago) Cómo eliminar los datos históricos. Dicha eliminación es absolutamente necesaria para cumplir lo establecido en las PCI DSS. 	<p>Proveedor de software: Proporcione la herramienta o el procedimiento para que los clientes puedan eliminar con seguridad los datos almacenados por versiones anteriores de acuerdo con el requisito 1.1.4. de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Borre todos los datos históricos de acuerdo con la <i>Guía de implementación de las PA-DSS</i> y el requisito 1.1.4 de las PA-DSS.</p>
1.1.5	Borre todos los datos confidenciales de autenticación (autorización previa) reunidos como consecuencia del proceso de resolución de problemas de la aplicación de pago.	<ul style="list-style-type: none"> Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3 establecidos a continuación. Dichos datos deben ser almacenados solamente en ubicaciones específicas, conocidas y con acceso limitado. Reúna sólo una cantidad limitada de datos necesarios para resolver un problema específico. Los datos confidenciales de autenticación se deben cifrar en el momento de almacenarlos. Dichos datos se deben borrar de manera segura e inmediatamente después de utilizarlos. 	<p>Proveedor de software: Resuelva los problemas del cliente de acuerdo con el requisito 1.1.5.a. de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Resuelva todos los problemas de acuerdo con la <i>Guía de implementación de las PA-DSS</i> y el requisito 1.1.5.a. de las PA-DSS.</p>
2.1	Purgue los datos de titulares de tarjetas después del período de retención definido por el cliente.	<ul style="list-style-type: none"> Los datos de titulares de tarjetas se deben purgar después de superar el período de retención definido por el cliente. Todas las ubicaciones en que la aplicación de pago almacena datos de titulares de tarjetas. 	<p>Proveedor de software: Infórmeles a los clientes que deben purgar los datos de titulares de tarjetas que superen los períodos de retención definidos por el cliente y las ubicaciones donde la aplicación de pago almacene dichos datos.</p> <p>Clientes y revendedores/integradores: Purgue los datos de titulares de tarjetas que superen el período de retención definido por el cliente.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
2.5	Proteja las claves utilizadas para asegurar los datos de los titulares de tarjeta contra divulgación o uso indebido.	<ul style="list-style-type: none"> ▪ Restrinja el acceso a las claves al número mínimo de custodios necesarios. ▪ Guarde las claves de forma segura en la menor cantidad de ubicaciones y formas posibles. 	<p>Proveedor de software: Infórmeles a los clientes que deben guardar las claves utilizadas para los datos de titulares de tarjeta en la menor cantidad de ubicaciones posibles, y que el acceso a las claves debe estar restringido a la menor cantidad de custodios posibles.</p> <p>Clientes y revendedores/integradores: Guarde las claves de forma segura en la menor cantidad de ubicaciones y restrinja el acceso a las claves a la menor cantidad de custodios posibles.</p>
2.6	Implemente los procesos y los procedimientos de gestión de claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas.	<ul style="list-style-type: none"> ▪ Cómo generar, distribuir, proteger, cambiar, almacenar y retirar/reemplazar claves de cifrado, cuando los clientes o revendedores/integradores participen en estas actividades de gestión de claves. ▪ Un formulario de Custodio de claves para que los custodios de las claves reconozcan que entienden y aceptan sus responsabilidades. ▪ Cómo realizar las funciones de gestión de claves que se definen abajo en los requisitos 2.6.1 hasta 2.6.7 de las PA- DSS. 	<p>Proveedor de software: Infórmeles a los clientes que acceden a claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas que implementen procesos y procedimientos de gestión de claves.</p> <p>Clientes y revendedores/integradores: Implemente los procesos y los procedimientos de gestión de claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 2.6 de las PA-DSS.</p>
2.7	Haga que no se pueda recuperar ningún material de clave criptográfica o criptograma almacenado por las versiones anteriores de la aplicación de pago.	<ul style="list-style-type: none"> ▪ El material criptográfico debe quedar irrecuperable. ▪ Cómo impedir que el material criptográfico pueda ser recuperado. ▪ Dicha incapacidad para recuperar el material es absolutamente necesaria para cumplir con las PCI. ▪ Cómo volver a cifrar datos históricos con claves nuevas. 	<p>Proveedor de software: Proporcione la herramienta o el procedimiento para eliminar con seguridad el material clave criptográfico o los criptogramas almacenados por las versiones anteriores, de conformidad con el requisito 1.1.5 de las PA-DSS y facilite la herramienta o el procedimiento para volver a cifrar los datos históricos con nuevas claves.</p> <p>Clientes y revendedores/integradores: Borre todo el material criptográfico histórico de acuerdo con la <i>Guía de implementación de las PA-DSS</i> y el requisito 1.1.5 de las PA-DSS.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
3.1	Utilice ID de usuario únicos y una autenticación segura, tanto para el acceso administrativo como para el acceso a datos de titulares de tarjetas.	<ul style="list-style-type: none"> ▪ Que la aplicación de pago aplica autenticación segura para todas las credenciales de autenticación que genera la aplicación al: <ul style="list-style-type: none"> – Aplicar los cambios seguros a las credenciales de autenticación una vez que finaliza la instalación y a cualquier cambio subsiguiente (después de la instalación) de conformidad con los requisitos 3.1.1 hasta 3.1 de las PA-DSS. ▪ Asigne una autenticación segura a las cuentas predeterminadas (incluso si estas no se utilizan) y desactive o no utilice las cuentas. ▪ Cómo cambiar y crear credenciales de autenticación cuando esas credenciales no son generadas ni gestionadas por la aplicación de pago, de acuerdo con los requisitos 8.5.8 hasta 8.5.15 de las PCI DSS, al concluir la instalación y para cambios subsiguientes después de la instalación, para todas las cuentas a nivel de aplicación con acceso administrativo y para todo acceso a datos de titulares de tarjeta. 	<p>Proveedor de software: Cuando la aplicación de pago genera o gestiona credenciales de autenticación, asegure que la aplicación de pago exija el uso de ID de usuario únicos y autenticación segura para cuentas/contraseña de la aplicación de pago, de conformidad con los requisitos 3.1.1 hasta 3.1.10 de las PA-DSS.</p> <p>Cuando las credenciales de autenticación no son generadas o gestionadas por la aplicación de pago, asegure que la <i>Guía de implementación de las PA-DSS</i> brinda a los clientes y revendedores/integradores orientación clara y precisa sobre cómo cambiar y crear credenciales de autenticación seguras de conformidad con los requisitos 3.1.1 hasta 3.1.10 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga ID de usuario únicos y una autenticación segura de acuerdo con la <i>Guía de implementación de las PA-DSS</i> y los requisitos 3.1.1 hasta 3.1.10 de las PA-DSS.</p>
3.2	Utilice ID de usuario únicos y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago.	Utilice nombres de usuario únicos y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago y/o datos de titulares de tarjetas de acuerdo con los requisitos 3.1.1 a 3.1.10 de las PA-DSS.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice ID de usuario únicos y una autenticación segura para las cuentas/contraseñas (cuando estén determinadas por el proveedor) a fin de acceder a computadoras, servidores y bases de datos según los requisitos 3.1.2 a 3.1.9 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga ID de usuario únicos y una autenticación segura de acuerdo con la <i>Guía de implementación de las PA-DSS</i> y los requisitos 3.1.2 hasta 3.1.10 de las PA-DSS.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
4.1	Implemente pistas de auditoría automatizadas.	<ul style="list-style-type: none"> ▪ Establezca valores de configuración del registro que cumplan con las PA-DSS, según los requisitos 4.2, 4.3 y 4.4 de las PCI DSS. ▪ Se deben activar los registros, ya que desactivarlos provocará un incumplimiento de las PCI DSS. 	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice registros compatibles de acuerdo con los requisitos 4.2, 4.3 y 4.4 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga registros que cumplan con las PCI DSS de conformidad con la <i>Guía de implementación de las PA-DSS</i> y los requisitos 4.2, 4.3 y 4.4 PA-DSS.</p>
4.4	Facilite el registro centralizado.	Proporcione instrucciones y procedimientos para incorporar los registros de la aplicación de pago a un servidor de registro centralizado.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita registro centralizado en entornos de cliente se conformidad con el requisito 4.4 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga registro centralizado de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 4.4 de las PA-DSS.</p>
5.4	Utilice sólo servicios, protocolos, componentes y software y hardware dependientes necesarios y seguros, incluyendo los proporcionados por terceros.	Documente todos los protocolos, servicios, componentes y software y hardware dependientes requeridos que sean necesarios para cualquier funcionalidad de la aplicación de pago.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice sólo protocolos, servicios, etc., necesarios, al 1) tener sólo protocolos, servicios, etc., necesarios, establecidos simples por opción predeterminada, 2) tener esos protocolos, servicios, etc., necesarios, configurados de forma segura por opción predeterminada, y 3) al documentar protocolos, servicios, etc., necesarios, como referencia para clientes y revendedores/integradores.</p> <p>Clientes y revendedores/integradores: Utilice la lista documentada de la <i>Guía de implementación</i> para que sólo se utilicen en el sistema protocolos, servicios, etc., necesarios y seguros, de conformidad con el requisito 5.4. de las PA-DSS.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
6.1	Implemente tecnología inalámbrica de manera segura.	<p>Si se utiliza tecnología inalámbrica dentro del entorno de pago:</p> <ul style="list-style-type: none"> ▪ Cambie los valores predeterminados del proveedor de servicio inalámbrico, incluyendo claves de cifrado inalámbrico, contraseñas y cadenas comunitarias SNMP ▪ Instale un firewall: <ul style="list-style-type: none"> - Entre redes inalámbricas y sistemas que almacenan datos de titulares de tarjetas, y - Configúrelo para negar y controlar (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde el entorno inalámbrico hacia el entorno del titular de la tarjeta. 	<p>Proveedor de software: Asesore a los clientes y revendedores/integradores para que, de conformidad con el requisito 6.1 de las PA-DSS, cambien los valores de configuración predeterminados del proveedor de tecnología inalámbrica cuando se utilice esta tecnología con la aplicación de pago.</p> <p>Cientes y revendedores/integradores: Para la tecnología inalámbrica implementada por clientes o revendedores/integradores dentro del entorno de pagos, cambie los valores de configuración predeterminados del proveedor e instale un firewall según la Guía de implementación de las PA-DSS y el requisito 2.1.1 de las PCI DSS.</p>
6.2	Asegure las transmisiones de datos de titulares de tarjetas que se realizan mediante redes inalámbricas.	Si la aplicación de pago se implementa dentro de un entorno inalámbrico, utilice las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) para implementar cifrado sólido para autenticación y transmisión de datos de titulares de tarjetas.	<p>Proveedor de software: Asesore a los clientes y revendedores/integradores para que, de conformidad con el requisito 6.2 de las PA-DSS, implementen transmisiones cifradas seguras, en caso de que se utilice tecnología inalámbrica con la aplicación de pago.</p> <p>Cientes y revendedores/integradores: Para la tecnología inalámbrica implementada en el entorno de pagos por clientes o revendedores/integradores, utilice transmisiones cifradas seguras de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 6.2 de las PA-DSS.</p>
9.1	Almacene datos de titulares de tarjetas únicamente en los servidores que no estén conectados a Internet.	No almacene datos de titulares de tarjetas en sistemas a los que se pueda acceder desde Internet (por ejemplo, el servidor web y el servidor de base de datos no deben estar en el mismo servidor).	<p>Proveedor de software: Asegúrese de que la aplicación de pago no requiera el almacenamiento de datos en la DMZ ni en sistemas accesibles desde Internet, ni permita el uso de una DMZ de conformidad con el requisito 9 de las PA-DSS.</p> <p>Cientes y revendedores/integradores: Establezca y mantenga las aplicaciones de pago de manera que los datos de titulares de tarjetas no se almacenen en sistemas a los que se pueda acceder desde Internet, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 9 de las PA-DSS.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
10.2	Implemente una autenticación de dos factores para el acceso remoto a la aplicación de pago.	Utilice una autenticación de dos factores (ID de usuario y contraseña, además de un rubro de autenticación adicional, como un token) si es posible acceder a la aplicación de pago de manera remota.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice una autenticación de dos factores, de conformidad con el requisito 10.2 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga una autenticación de dos factores para el acceso remoto a la aplicación de pago, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 10.2 de las PA-DSS.</p>
10.3.1	Entregue de manera segura las actualizaciones de la aplicación de pago.	<ul style="list-style-type: none"> ▪ Active tecnologías de acceso remoto para actualizaciones de la aplicación de pago sólo cuando sea necesario para descargas, y desactívelas de inmediato después de terminar las descargas, de conformidad con el requisito 12.3.9 de las PCI DSS. ▪ Si la computadora está conectada mediante una VPN u otra conexión de alta velocidad, reciba actualizaciones remotas de la aplicación de pago por medio de un firewall o un firewall personal configurado de forma segura, de conformidad con el requisito 1 de las PCI DSS. 	<p>Proveedor de software: Entregue de manera segura las actualizaciones de la aplicación de pago de forma segura de conformidad con el requisito 10.3 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Reciba de manera segura de parte del proveedor las actualizaciones de la aplicación de pago, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 10.3 de las PA-DSS y el requisito 1 de las PCI DSS.</p>
10.3.2	Implemente de manera segura un software de acceso remoto.	Implemente y utilice funciones de seguridad del software de acceso remoto en caso de utilizarlo para acceder de manera remota a la aplicación de pago o al entorno de pago.	<p>Proveedor de software: (1) Si el proveedor utiliza productos de acceso remoto para acceder a sitios de clientes, utilice las funciones de seguridad de acceso remoto, como las que se especifican en el requisito 10.3.2 de las PA-DSS. (2) Asegúrese de que la aplicación de pago admita que el cliente utilice funciones de seguridad de acceso remoto.</p> <p>Clientes y revendedores/integradores: Utilice funciones de seguridad de acceso remoto, si usted permite el acceso remoto a las aplicaciones de pago, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 10.3.2 de las PA-DSS.</p>

PA-DSS Requisito	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
11.1	Asegure las transmisiones de datos de titulares de tarjetas que se realizan mediante redes públicas.	Implemente y utilice cifrado sólido y protocolos de seguridad para la transmisión segura de datos de titulares de tarjetas mediante redes públicas.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice cifrado sólido y protocolos de seguridad para transmisiones de datos de titulares de tarjetas mediante redes públicas, de conformidad con el requisito 11.1 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Establezca y mantenga cifrado sólido y protocolos de seguridad para transmisiones seguras de datos de titulares de tarjetas, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 11.1 de las PA-DSS.</p>
11.2	Cifre los datos de titulares de tarjetas por medio de tecnologías de mensajería de usuario final.	Implemente y utilice una solución que deje el PAN ilegible o implemente cifrado sólido si los PAN no se pueden enviar con tecnologías de mensajería de usuario final.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente cifre o deje ilegible los PAN en caso de enviarlos por medio de tecnologías de mensajería de usuario final, de conformidad con el requisito 11.2 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Cifre todos los PAN enviados por medio de tecnologías de mensajería de usuario final, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 11.2 de las PA-DSS.</p>
12.1	Cifre el acceso administrativo que no sea de consola.	Implemente y utilice cifrado sólido (como SSH, VPN, o SSL/TLS) para el cifrado de todo acceso administrativo que no sea de consola a la aplicación de pago o servidores que se encuentran en el entorno de datos de titulares de tarjetas.	<p>Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente cifre todo acceso administrativo que no sea de consola, de conformidad con el requisito 12.1 de las PA-DSS.</p> <p>Clientes y revendedores/integradores: Cifre todo el acceso administrativo que no sea de consola, de conformidad con la <i>Guía de implementación de las PA-DSS</i> y el requisito 12.1 de las PA-DSS.</p>

Anexo B: Confirmación de la configuración del laboratorio de pruebas específica de la evaluación de las PA-DSS

Para: *Proveedor de software Nombre de la aplicación Número de versión*

Para cada evaluación según las PA-DSS que se lleve a cabo, el PA-QSA debe completar este documento a fin de confirmar el estado y las capacidades del laboratorio utilizado para llevar a cabo las pruebas de la evaluación de las PA-DSS. Una vez que se haya completado este documento, se deberá presentar junto con el documento completo de *Procedimientos de Auditoría de Seguridad de las PA-DSS*.

Para cada procedimiento de validación del laboratorio, utilice las columnas tituladas “Completado en el laboratorio del PA-QSA” o “Completado en el laboratorio del proveedor” para indicar si el laboratorio utilizado para la evaluación y el laboratorio que se somete a estos procedimientos de validación fue el laboratorio del PA-QSA o el laboratorio del proveedor de software.

Describa la arquitectura de las pruebas del laboratorio y el entorno implementado para esta revisión según las PA-DSS:

Describa cómo se simuló, para esta revisión según las PA-DSS, el uso real de la aplicación de pago en el laboratorio:

Requisito del laboratorio	Procedimiento de validación del laboratorio	Completado en		Comentarios
		Laboratorio de PA-QSA	Laboratorio del proveedor	
1. Instale la aplicación de pago según las instrucciones de instalación del proveedor o según la capacitación provista al cliente.	1. Verifique que el manual de instalación del proveedor o la capacitación provista a los clientes se haya utilizado para realizar la instalación predeterminada para el producto de la aplicación de pago en todas las plataformas enumeradas en el informe de PA-DSS.	<input type="checkbox"/>	<input type="checkbox"/>	
2. Instale y pruebe todas las versiones de la aplicación de pago publicadas en el informe de PA-DSS.	2.a Verifique que se hayan instalado todas las implementaciones comunes (incluidas las versiones específicas de cada región/país) de la aplicación de pago que se deberá probar.	<input type="checkbox"/>	<input type="checkbox"/>	
	2.b Verifique que se hayan probado todas las versiones y plataformas de la aplicación de pago.	<input type="checkbox"/>	<input type="checkbox"/>	

Requisito del laboratorio	Procedimiento de validación del laboratorio	Completado en		Comentarios
		Laboratorio de PA-QSA	Laboratorio del proveedor	
	2.c Verifique que se hayan probado todas las funciones de la aplicación de pago.	<input type="checkbox"/>	<input type="checkbox"/>	
3. Instale e implemente todos los dispositivos de seguridad requeridos por las PCI DSS.	3. Verifique que se hayan implementado todos los dispositivos de seguridad requeridos por las PCI DSS (por ejemplo, los firewalls y el software antivirus) en los sistemas de prueba.	<input type="checkbox"/>	<input type="checkbox"/>	
4. Instale y/o configure todos los valores de configuración de seguridad requeridos por las PCI DSS.	4. Verifique que se hayan implementado todos los valores de configuración, parches, etc., del sistema que cumplan con las PCI DSS en los sistemas de prueba para los sistemas operativos, el software del sistema y las aplicaciones utilizadas por la aplicación de pago.	<input type="checkbox"/>	<input type="checkbox"/>	
5. Simule el uso real de la aplicación de pago.	5.a El laboratorio simula el uso real de la aplicación de pago, incluidos todos los sistemas y las aplicaciones en los que se implementará la aplicación de pago. Por ejemplo, una implementación estándar de una aplicación de pago podría incluir un entorno de cliente/servidor dentro de un local minorista con una máquina POS y una red corporativa o gestión operativa. El laboratorio simula la implementación total.	<input type="checkbox"/>	<input type="checkbox"/>	
	5.b El laboratorio utiliza solo los números de tarjeta de prueba para la simulación/prueba; no se utilizan PAN activos para las pruebas. <i>Nota: Las tarjetas de prueba se pueden obtener del proveedor o de un procesador o adquirente.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.c El laboratorio ejecuta las funciones de autorización y/o liquidación de la aplicación de pago y se examinan los resultados según el punto 6 que aparece más adelante.	<input type="checkbox"/>	<input type="checkbox"/>	

Requisito del laboratorio	Procedimiento de validación del laboratorio	Completado en		Comentarios
		Laboratorio de PA-QSA	Laboratorio del proveedor	
	5.d El laboratorio y/o los procesos hacen un mapa de los resultados generados por la aplicación de pago para cada escenario posible, ya sea temporal, permanente, procesamiento de errores, modo de depuración, archivos de registro, etc.	<input type="checkbox"/>	<input type="checkbox"/>	
	5.e El laboratorio y/o los procesos simulan y validan todas las funciones de la aplicación de pago, para incluir la generación de todas las condiciones de error y las entradas de registro utilizando los datos activos simulados como los datos inválidos.	<input type="checkbox"/>	<input type="checkbox"/>	
6. Proporcione las capacidades para las siguientes metodologías de pruebas de penetración y de uso de pruebas:	6.a Uso de herramientas o métodos forenses: Las herramientas o los métodos forenses se utilizaron para buscar los resultados identificados para obtener evidencias de datos confidenciales de autenticación (herramientas comerciales, secuencias de comandos, etc.), según el requisito 1.1.1 a 1.1.3 de las PA-DSS. ⁴	<input type="checkbox"/>	<input type="checkbox"/>	
	6.b Intente aprovechar las vulnerabilidades de las aplicaciones: Se utilizaron vulnerabilidades actuales (por ejemplo, el OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), para intentar explotar las aplicaciones de pago, de conformidad con el requisito 5.2 de las PA-DSS.	<input type="checkbox"/>	<input type="checkbox"/>	
	6.c El laboratorio y/o los procesos destinados a ejecutar un código arbitrario durante el proceso de actualización de la aplicación de pago: Ejecute el proceso de actualización con un código arbitrario según el requisito 7.2.b de las PA-DSS.	<input type="checkbox"/>	<input type="checkbox"/>	

⁴ Herramienta o método forense: Herramienta o método para descubrir, analizar y presentar datos forenses, que brinda una manera sólida de autenticar, buscar y recuperar evidencia informática con rapidez y de modo exhaustivo. En el caso de las herramientas o los métodos forenses que utilizan los PA-QSA, tales herramientas o métodos deben localizar con precisión los datos confidenciales de autenticación escritos por la aplicación de pago. Estas herramientas pueden ser comerciales, de código abierto o desarrolladas para uso interno por el PA-QSA.

Requisito del laboratorio	Procedimiento de validación del laboratorio	Completado en		Comentarios
		Laboratorio de PA-QSA	Laboratorio del proveedor	
7. Utilice el laboratorio del proveedor ÚNICAMENTE después de verificar que se cumplan todos los requisitos.	7.a Si se necesita utilizar el laboratorio del proveedor de software (por ejemplo, el PA-QSA no cuenta con el sistema mainframe, AS400, ni el Tandem en el que se ejecuta la aplicación de pago), el PA-QSA puede: (1) utilizar a préstamo el equipo del proveedor, o (2) utilizar las instalaciones del laboratorio del proveedor, siempre que esto se detalle en el informe junto con la ubicación de las pruebas. Para cualquiera de las dos opciones, el PA-QSA debe verificar que el equipo y el laboratorio del proveedor cumplan con los siguientes requisitos:	<input type="checkbox"/>	<input type="checkbox"/>	
	7.b El PA-QSA debe verificar que el laboratorio del proveedor cumpla con todos los requisitos antes mencionados y especificados en el documento, y debe documentar los detalles del informe.	<input type="checkbox"/>	<input type="checkbox"/>	
	7.c El PA-QSA debe validar la instalación adecuada del entorno de laboratorio para asegurarse de que éste simule fielmente una situación real y que el proveedor no haya modificado o alterado el entorno de ninguna manera.	<input type="checkbox"/>	<input type="checkbox"/>	
	7.d Todas las pruebas deben ser ejecutadas por el PA-QSA (el proveedor no puede ejecutar pruebas respecto de su propia aplicación).	<input type="checkbox"/>	<input type="checkbox"/>	
	7.e Todas las pruebas (1) serán realizadas in situ en el local del proveedor, o (2) serán realizadas de manera remota mediante una conexión de red utilizando un vínculo seguro (por ejemplo, una VPN).	<input type="checkbox"/>	<input type="checkbox"/>	
	7.f Utilice únicamente números de tarjetas de prueba para simulación/prueba; no utilice PAN activos para las pruebas. Estas tarjetas de prueba se pueden obtener del proveedor o de un procesador o adquirente.	<input type="checkbox"/>	<input type="checkbox"/>	

Requisito del laboratorio	Procedimiento de validación del laboratorio	Completado en		Comentarios
		Laboratorio de PA-QSA	Laboratorio del proveedor	
8. Mantenga un proceso eficiente del control de calidad (QA)	8.a El personal de QA del PA-QSA debe verificar que se incluyan todas las plataformas identificadas en el informe de PA-DSS que aparece en las pruebas.	<input type="checkbox"/>	<input type="checkbox"/>	
	8.b El personal de QA del PA-QSA debe verificar que se prueben todos los requisitos de las PA-DSS.	<input type="checkbox"/>	<input type="checkbox"/>	
	8.c El personal de QA del PA-QSA debe verificar que las configuraciones y los procesos del laboratorio del PA-QSA cumplan con los requisitos y se documenten con precisión en el informe.	<input type="checkbox"/>	<input type="checkbox"/>	
	8.d El personal de QA del PA-QSA debe verificar que el informe muestre con precisión los resultados de las pruebas.	<input type="checkbox"/>	<input type="checkbox"/>	