Industria de tarjetas de pago (PCI)

Norma de seguridad de datos para las aplicaciones de pago

Requisitos y procedimientos de evaluación de seguridad

Versión 3.2

Mayo de 2016

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción	Páginas
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 Atestación 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”.*	
Noviembre de 2013	3.0	Actualización de la PA-DSS, versión 2. Para conocer en detalle los cambios, consulte *“PA-DSS – Resumen de cambios de las PA-DSS versión 2.0 a 3.0”.*	
Mayo de 2015	3.1	Actualización de la PA-DSS, versión 3.0. Para conocer en detalle los cambios, consulte *PA-DSS – Resumen de cambios de la PA-DSS* versión 3.0 a 3.1.	
Mayo de 2016	3.2	Actualización de la PA-DSS, versión 3.1. Para obtener los detalles, consulte *PA-DSS - Resumen de cambios de la PA-DSS versión 3.1 a 3.2*	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Índice

Modificaciones realizadas a los documentos ... 2
Introducción ... 5
Finalidad de este documento ... 5
Relación entre PCI DSS y PA-DSS ... 5
Integradores y revendedores ... 7
Información sobre la aplicabilidad de las PCI DSS ... 7
Alcance de las PA-DSS ... 9
Aplicabilidad de las PA-DSS a las aplicaciones de pago en terminales de hardware ... 10
Guía de implementación de las PA-DSS ... 12
Requisitos del Asesor de Seguridad Certificado para las Aplicaciones de Pago (PA-QSA) ... 13
Laboratorio de pruebas ... 13
Instrucciones y contenido para el informe de validación ... 13
Pasos para completar las PA-DSS ... 14
Guía del programa PA-DSS ... 14
Requisitos y procedimientos de evaluación de seguridad de las PA-DSS ... 15
Requisito 1: *No retenga el contenido completo de la pista, el código o valor de verificación de la tarjeta (CAV2, CID, CVC2, CVV2) ni los datos de bloqueo del PIN* ... 16
Requisito 2: *Proteger los datos almacenados del titular de la tarjeta* ... 22
Requisito 3: *Proporcione funciones de autenticación segura* ... 31
Requisito 4: *Registre la actividad de la aplicación de pago* ... 42
Requisito 5: *Desarrolle aplicaciones de pago seguras* ... 46
Requisito 6: *Proteja las transmisiones inalámbricas* ... 67
Requisito 7: *Evalúe las aplicaciones de pago para corregir las vulnerabilidades y para mantener las actualizaciones de la aplicación* ... 71
Requisito 8: *Facilite la implementación de una red segura* ... 75
Requisito 9: *Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet* ... 77
Requisito 10: *Facilite un acceso remoto seguro a la aplicación de pago* ... 79
Requisito 11: *Cifre el tráfico sensitivo de las redes públicas* ... 83
Requisito 12: *Cifre el acceso administrativo que no sea de consola* ... 86
Requisito 13: *Mantenga una Guía de implementación de las PA-DSS para los clientes, revendedores e integradores* ... 88

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 14: *Asigne responsabilidades según las PA-DSS al personal y establezca programas de capacitación para el personal, los clientes, los revendedores y los integradores* 90
Anexo A: Resumen de contenidos para la *Guía de implementación de las PA-DSS* 93
Anexo B: Configuración del laboratorio de pruebas para la evaluación de las PA-DSS 111

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Introducción

Finalidad de este documento

Los requisitos de las PA-DSS (normas de seguridad de datos para las aplicaciones de pago) y los procedimientos de evaluación de seguridad de la PCI (industria de tarjetas de pago) definen los requisitos de seguridad y los procedimientos de evaluación de los proveedores de software de aplicaciones de pago. Los PA-QSA (asesores de seguridad certificados para aplicaciones de pago), quienes realizan las evaluaciones de las aplicaciones de pago, utilizarán este documento para validar que una aplicación de pago cumpla con las PA-DSS. Para obtener más información sobre cómo documentar evaluaciones según las PA-DSS y crear el ROV (informe de validación), los PA-QSA deben consultar la *Plantilla para crear informes ROV según las PA-DSS,* disponible en el sitio web del PCI SSC (PCI Security Standards Council) en www.pcisecuritystandards.org.

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 sola no implica que una entidad cumpla con las PCI DSS (normas de seguridad de datos de la industria de tarjetas de pago), 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). Los requisitos de las PA-DSS se derivan de los requisitos de las *PCI DSS (normas de seguridad de datos de la industria de tarjetas de pago) y de los procedimientos de evaluación de seguridad*, que detallan lo necesario 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). Las PCI DSS se pueden ver en www.pcisecuritystandards.org.

Todas las aplicaciones que almacenan, procesan o transmiten datos de titulares de tarjetas se encuentran dentro del ámbito de aplicación para la evaluación de las PCI DSS de una entidad, incluidas las aplicaciones que hayan sido validadas según las PA-DSS. La evaluación de las PCI DSS debe controlar que la aplicación de pago que cumple con las PA-DSS esté configurada correctamente e implementada de manera segura de acuerdo con los requisitos de las PCI DSS. Si una aplicación de pago ha sufrido cambios de personalización, requerirá una revisión más exhaustiva durante la evaluación de las PCI DSS, dado que la aplicación puede haber dejado de representar la versión que fuera validada por la PA-DSS.

Es posible que las PCI DSS no se apliquen directamente a proveedores de aplicaciones de pago, a menos que el proveedor almacene, procese o transmita datos del titular de la tarjeta, o tenga acceso a los datos del titular de la tarjeta de sus clientes. Sin embargo, dado que los clientes de los proveedores de las aplicaciones de pago son quienes se valen de estas para almacenar, procesar y transmitir datos del titular de la tarjeta y son ellos quienes deben cumplir con las PCI DSS; por lo tanto, las aplicaciones de pago deben facilitar, y no entorpecer, el cumplimiento de las PCI DSS por parte de los clientes. Estas son algunas de las maneras en que las aplicaciones de pago inseguras pueden impedir el cumplimiento:

1. Almacenamiento de datos de banda magnética o de datos equivalentes que están el chip en la red del cliente después de la autorización;

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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 el PAN (número de cuenta principal), el contenido completo de la pista, los códigos y valores de verificación de la tarjeta (CAV2, CID, CVC2, CVV2), los PIN y los bloqueos de PIN, como el fraude perjudicial derivado de tales fallos de seguridad.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Integradores y revendedores

Los proveedores de aplicaciones pueden contratar a integradores o revendedores para vender, instalar o mantener aplicaciones de pago en su nombre. La función de los integradores o revendedores es verificar la instalación y el funcionamiento de las aplicaciones de pago de modo seguro, dado que prestan servicios en el sitio a los clientes del proveedor y asisten con la instalación de las aplicaciones de pago validadas según las PA-DSS. Si la configuración, el mantenimiento o la compatibilidad de una aplicación no se realizan correctamente, podrían presentarse vulnerabilidades en la seguridad del entorno de datos del titular de la tarjeta, que luego podrían aprovechar los atacantes. Los proveedores de aplicaciones deben orientar a los clientes, integradores y revendedores sobre cómo instalar y configurar las aplicaciones de pago para que cumplan con lo establecido en las PCI DSS.

El PCI SSC (PCI Security Standards Council) capacita a los QIR (integradores y revendedores certificados por PCI) en las PCI DSS y en las PA-DSS para que puedan implementar aplicaciones de pago de modo seguro. Para obtener más información sobre el programa para QIR (integradores y revendedores certificados por PCI), consulte en www.pcisecuritystandards.org.

Información sobre la aplicabilidad de las PCI DSS

La PCI DSS se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a ***todas*** las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta y/o datos confidenciales de autenticación.

Los datos del titular de la tarjeta y los datos de autenticación confidenciales se definen de la siguiente manera:

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

El PAN (número de cuenta principal) es el factor que define los datos del titular de la tarjeta. Si el nombre del titular de tarjeta, el código de servicio y/o la fecha de vencimiento se almacenan, procesan o transmiten con el PAN (número de cuenta principal) o se encuentran presentes de algún otro modo en el entorno de datos del titular de la tarjeta, se deben proteger de conformidad con los requisitos aplicables de la PCI DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

La tabla que aparece en la siguiente página ilustra los elementos que habitualmente se utilizan de los datos del titular de la tarjeta y los datos de autenticación confidenciales, independientemente de que esté permitido o prohibido almacenar dichos datos y 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	Datos almacenados ilegibles según el Requisito 2.3 de las PA-DSS
Datos de cuentas	**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]	Contenido completo de la pista [2]	No	No se puede almacenar según el Requisito 1.1 de las PA-DSS.
		CAV2/CVC2/CVV2/CID[3]	No	No se puede almacenar según el Requisito 1.1 de las PA-DSS.
		PIN/Bloqueo de PIN[4]	No	No se puede almacenar según el Requisito 1.1 de las PA-DSS.

Los Requisitos 2.2 y 2.3 de las PA-DSS solo se aplican al PAN. Si el PAN (número de cuenta principal) se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN (número de cuenta principal) debe ser ilegible de acuerdo con el Requisito 2.3 de las PA-DSS.

No se deben almacenar los datos confidenciales de autenticación después de la autorización, incluso si están cifrados. Esto se implementa aún cuando no haya PAN en el entorno.

---

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

2 *Contenido completo de la pista que se encuentra en la banda magnética, datos equivalentes que se encuentran en el chip o en cualquier otro dispositivo*

3 *La cifra de tres o cuatro dígitos en el anverso o reverso de la tarjeta de pago*

4 *El número de identificación personal ingresado por el titular de la tarjeta durante una transacción con tarjeta presente o el bloqueo de PIN cifrado presente en el mensaje de la transacción.*

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Alcance de las PA-DSS

Las PA-DSS se aplican a proveedores de software y a otros que desarrollan aplicaciones de pago y que almacenan, procesan o transmiten datos del titular de la tarjeta o datos de autenticación confidenciales. Para obtener más información sobre la elegibilidad de los diferentes tipos de aplicaciones, consulte la *Guía del programa PA-DSS*.

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

- Cobertura de toda la funcionalidad de la aplicación de pago, incluidas, entre otras, las siguientes:
  1) Las funciones de pago completas (autorización y liquidación).
  2) Las entradas y las salidas de datos.
  3) Las condiciones de error.
  4) Las interfaces y las conexiones con otros archivos, sistemas 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.
  7) Los mecanismos de autenticación.
- Cobertura del asesoramiento que el proveedor de aplicaciones de pago debe proporcionarles a los clientes y a los integradores/revendedores (consulte la *Guía de implementación de las PA-DSS* más adelante en este documento) para garantizar lo siguiente:
  1) El cliente sepa cómo implementar la aplicación de pago de conformidad con las PCI DSS.
  2) El cliente debe saber con claridad que determinadas configuraciones del entorno y de la aplicación de pago pueden impedir que se cumplan las PCI DSS.

  Tenga en cuenta que es posible que el proveedor de aplicaciones de pago deba proporcionar dicho asesoramiento incluso cuando la configuración específica:
  1) No pueda ser controlada por el proveedor de aplicaciones de pago después de que el cliente haya instalado la aplicación.
  2) Sea responsabilidad del cliente y no, del proveedor de aplicaciones de pago.
- "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.)"
- 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.)

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

- Cobertura de todos los componentes de software relacionados con la aplicación de pago, incluidos los requisitos y las dependencias de software de terceros.
- Cobertura de cualquier otro tipo de aplicación de pago necesario para una implementación completa.
- Cobertura de metodología de control de versiones del proveedor.
-

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

Esta sección proporciona asesoramiento para los proveedores que deseen obtener validación según las PA-DSS para aplicaciones de pago residentes en terminales de hardware (también conocidos como terminales de pago independientes o dedicadas).

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 solo rige para las aplicaciones de pago que residan en un POI (dispositivo de punto de interacción) 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, los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) deben probar completamente la aplicación de pago con su hardware dependiente con respecto a todos los requisitos de las PA-DSS. Si los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) determinan que la aplicación de pago residente no puede cumplir con uno o más requisitos de las PA-DSS, pero que estos se satisfacen por medio de los controles validados conforme a PCI PTS, los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) deben tomar las siguientes medidas:

1. Documentar claramente cuáles requisitos se cumplen de conformidad con las PA-DSS (como de costumbre);

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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 (asesor de seguridad certificado para las aplicaciones de pago) 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 una 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 o el integrador/revendedor debe empaquetar la aplicación para su distribución de tal modo que esta 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.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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 e integradores/revendedores sobre la implementación segura de un producto, documentar los detalles específicos de configuración segura mencionados en este documento, así como delinear claramente las responsabilidades del proveedor, del integrador/revendedor y del cliente en el cumplimiento de los requisitos de las PCI DSS. Esta guía debe detallar la manera en que el cliente o el integrador/revendedor 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 las contraseñas de las PCI DSS, aún cuando no esté controlada por la aplicación de pago, a fin de que el cliente o el integrador/revendedor pueda entender cómo implementar contraseñas seguras para cumplir con lo establecido en las PCI DSS.

La *Guía de implementación de las PA-DSS* debe proporcionar detalles sobre cómo configurar las aplicaciones de pago para que cumplan con los requisitos, y no solo repetir los requisitos de las PCI DSS o las PA-DSS en otras palabras. Durante una evaluación, el PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe controlar que las instrucciones sean precisas y efectivas. Además, debe controlar que la *Guía de implementación de las PA-DSS* se distribuya entre los clientes y los integradores/revendedores.

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*.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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

Únicamente los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) empleados por las empresas de PA-QSA están autorizados para realizar las evaluaciones de las PA-DSS. Para obtener una lista de empresas calificadas para realizar evaluaciones de las PA-DSS, consulte la lista de los QSA de aplicaciones de pago 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.
- Los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) deben llenar y presentar el *Anexo B,* según el laboratorio específico utilizado para la aplicación de pago que está siendo revisada, como parte del ROV (informe de validación) completo de las PA-DSS.

Instrucciones y contenido para el informe de validación

Ahora, se proporcionan las instrucciones y el contenido del ROV (informe de validación) de las PA-DSS en la *Plantilla para crear informes de ROV según las PA-DSS.* Para crear un informe de validación, se debe usar la *Plantilla para crear informes ROV según las PA-DSS*. Solo se deben presentar ante el PCI SSC los ROV (informe de validación) que cumplan con los requisitos de las aplicaciones de pago. Para conocer en detalle el proceso de presentación del ROV (informe de validación), consulte la *Guía del programa PA-DSS*.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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: Configuración del laboratorio de pruebas 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 PA-QSA debe realizar lo siguiente:

1. Confirmar el alcance de la evaluación de las PA-DSS.
2. Llevar a cabo la evaluación de las PA-DSS.
3. Completar el ROV (informe de validación) usando la *Plantilla para crear informes ROV según las PA-DSS*, que incluye la confirmación de la configuración del laboratorio de pruebas que usará para la evaluación de las PA-DSS.
4. Completar y firmar una Atestación de validación (el PA-QSA y el proveedor de software). La Atestación de validación está disponible en el sitio web del PCI SSC (www.pcisecuritystandards.org).
5. Una vez completos, presente todos los documentos mencionados anteriormente y la *Guía de implementación de las PA-DSS* ante el PCI SSC de acuerdo con la *Guía del programa PA-DSS.*

Nota:

No deben presentarse las PA-DSS si no se han validado todos los requisitos como "implementados".

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:

- Detalles de las diferentes versiones de la PA-DSS y sus fechas de entrada en vigencia
- La aplicabilidad de las PA-DSS de acuerdo con los diferentes tipos de aplicaciones.
- 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 de pago validadas.
- 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.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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

A continuación, se definen los encabezados de las columnas de la tabla de requisitos de las PA-DSS y procedimientos de evaluación de seguridad:

- **Requisitos de las PA-DSS**: Esta columna define los requisitos de seguridad con los que se compararán las aplicaciones de pago para validarlas.
- **Procedimientos de pruebas**: Esta columna define los procedimientos de pruebas que deben seguir los PA-QSA a los efectos de validar que se cumplan los requisitos de las PA-DSS.
- **Guía**: Esta columna describe la intención o el objetivo de seguridad que justifica cada requisito de las PA-DSS y tiene por objetivo ayudar a comprender estos requisitos. La guía en esta columna no reemplaza ni modifica los requisitos de las PA-DSS ni de los procedimientos de pruebas.

Nota:

Los requisitos de las PA-DSS no se deben considerar "implementados" si alguno de los controles no se ha implementado aún o si están programados para completarse en el futuro.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 1: No retenga el contenido completo de la pista, el código o valor de verificación de la tarjeta (CAV2, CID, CVC2, CVV2) ni los datos de bloqueo del PIN

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
1.1 No almacene datos de autenticación confidenciales después de recibir la autorización (incluso cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización. Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 1.1.1 a 1.1.3 establecidos a continuación. ***Concuerda con el Requisito 3.2 de las PCI DSS***	**1.1.a** Si esta aplicación de pago almacena datos de autenticación confidenciales, verifique que la aplicación sea solamente para emisores de tarjetas de pago o empresas que respaldan los servicios de emisión.	Los datos de autenticación confidenciales consisten en el contenido completo de la pista, los códigos o valores de validación de la tarjeta y los datos de PIN. Se prohíbe el almacenamiento de datos de autenticación confidenciales después de la autorización. Estos datos son muy valiosos para las personas malintencionadas, ya que les permiten generar tarjetas de pago falsas y crear transacciones fraudulentas. Las entidades que emiten tarjetas de pago, que prestan o respaldan servicios de emisión crearán y controlarán, con frecuencia, los datos de autenticación confidenciales como parte de su tarea de emisión. Es posible que los emisores de tarjetas de pago y las empresas que respaldan los servicios de emisión almacenen datos de autenticación confidenciales si existe una justificación de negocio y los datos se almacenan de forma segura. Las entidades no emisoras no están autorizadas a retener datos de autenticación confidenciales después de la autorización y requieren de la aplicación para disponer de un mecanismo que les permita eliminar los datos de manera segura y lograr que sean irrecuperables.
	1.1.b Para todas las demás aplicaciones de pago, si los datos de autenticación confidenciales (consulte los puntos 1.1.1–1.1.3 a continuación) se almacenan antes de la autorización, obtenga y revise la metodología para eliminar los datos de manera segura a fin de controlar que sean irrecuperables.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
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. ***Nota:*** *En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:* • *El nombre del titular de la cuenta.* • *Número de cuenta principal (PAN).* • *Fecha de vencimiento.* • *Código de servicio* *Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.* ***Concuerda con el Requisito 3.2.1 de las PCI DSS***	**1.1.1** Instale la aplicación de pago y realice numerosas transacciones de prueba que simulen todas las funciones de la aplicación de pago, incluida la generación de todas las condiciones de error y las entradas de registro. Utilice las herramientas o métodos forenses (herramientas comerciales, secuencias de comandos, etc.)[5] 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 los datos equivalentes que estén en un chip no se almacenen después de la autorización. Incluya, al menos, los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago): • 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	Si se almacena el contenido completo de la pista, las personas malintencionadas que obtengan esos datos pueden reproducir tarjetas de pago y efectuar transacciones fraudulentas.

[5] *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.*

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
1.1.2 Después de la autorización, no almacene el valor o código de verificación de tarjetas (cifra de tres o cuatro dígitos impresa en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes. ***Concuerda con el Requisito 3.2.2 de las PCI DSS***	**1.1.2** Instale la aplicación de pago y efectúe numerosas transacciones de prueba que simulen todas las funciones de la aplicación de pago, incluida la generación de todas las condiciones de error y las entradas de registro. Utilice las herramientas 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, al menos, los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago): • 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	El propósito del código de validación de las tarjetas es proteger las transacciones que se efectúan de manera no presencial, ya sean transacciones por Internet o correo/teléfono (MO/TO), en las que ni el consumidor ni la tarjeta están presentes. Si se hurtan estos datos, las personas malintencionadas pueden efectuar transacciones fraudulentas por Internet y transacciones MO/TO (correo o teléfono).

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
1.1.3 Después de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado. ***Concuerda con el Requisito 3.2.3 de las PCI DSS***	**1.1.3** Instale la aplicación de pago y efectúe numerosas transacciones de prueba que simulen todas las funciones de la aplicación de pago, incluida la generación de todas las condiciones de error y las entradas de registro. Utilice las herramientas o métodos forenses (herramientas comerciales, secuencias 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, al menos, los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago). • 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	Sólo el propietario de la tarjeta o el banco emisor de la tarjeta deben conocer estos valores. Si se hurtan estos datos, personas malintencionadas pueden efectuar transacciones de débito basadas en PIN fraudulentas (por ejemplo, retiros de cajeros automáticos).

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
1.1.4 Borre de manera segura el contenido de la pista (de la banda magnética o los datos equivalentes que están en un chip), los valores o códigos de verificación 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. ***Nota:*** *Este requisito solamente se implementa cuando existen versiones anteriores de la aplicación de pago que hayan almacenado datos de autenticación confidenciales.* ***Concuerda con el Requisito 3.2 de las PCI DSS***	**1.1.4.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los integradores/revendedores: • Se deben eliminar los datos históricos (contenido de la pista, 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 las PCI DSS. **1.1.4.b** Consulte la documentación de la configuración y los archivos de software de la aplicación de pago para controlar que el proveedor proporcione una herramienta o un procedimiento de borrado seguro para eliminar los datos. **1.1.4.c** Compruebe que, mediante el uso de herramientas o métodos forenses, la herramienta o el procedimiento de borrado 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.	Después de la autorización, no está permitido almacenar estos elementos de datos de autenticación confidenciales. Si las versiones anteriores de las aplicaciones de pago almacenan esta información, el proveedor de la aplicación de pago debe proporcionar instrucciones en la *Guía de implementación de las PA-DS* y una herramienta o un procedimiento de borrado seguro. Si estos datos no se borran de manera segura, pueden permanecer ocultos en los sistemas del cliente, y personas malintencionadas que obtengan acceso a esta información pueden usarla para generar tarjetas de pago falsas o para efectuar transacciones fraudulentas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
1.1.5 No almacene datos de autenticación confidenciales en los sistemas del proveedor. En el caso de que se utilicen datos de autenticación confidenciales (datos previos a la autorización) con fines de depuración o resolución de problemas, asegúrese de tomar las siguientes medidas: • Recopile los datos de autenticación confidenciales solo cuando sea necesario para resolver un problema específico. • Almacene dichos datos en ubicaciones específicas y conocidas que tengan acceso limitado. • Recopile la menor cantidad de datos posible para resolver un problema específico. • Cuando almacene los datos de autenticación confidenciales, realícelo mediante una criptografía sólida. • Borre los datos de manera segura inmediatamente después de utilizarlos. Recuerde borrar los siguientes datos: - Archivos de registro. - Archivos de depuración. - Otras fuentes de datos que se reciben por parte de los clientes. ***Concuerda con el Requisito 3.2 de las PCI DSS***	**1.1.5.a** Examine los procedimientos del *proveedor del software* para resolver problemas de los clientes y compruebe que estos incluyan lo siguiente: • Recopilación de datos de autenticación confidenciales solo 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 datos de autenticación confidenciales cuando se almacenen. • Borrado seguro de dichos datos inmediatamente después de utilizarlos. **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. **1.1.5.c** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los integradores/revendedores: • 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.	Si el proveedor presta servicios a los clientes que puedan requerir la recolección de datos de autenticación confidenciales (por ejemplo, con fines de depuración o resolución de problemas), el proveedor debe asegurar la recolección mínima y segura, así como la eliminación de modo seguro de estos datos cuando ya no sean necesarios. Si la resolución de un problema requiere que la aplicación se configure temporalmente para capturar los SAD (datos de autenticación confidenciales), la aplicación se debe restablecer a su configuración segura usual (es decir, desactivar la recolección de SAD) inmediatamente después de completar la captura de datos necesarios. Cuando los SAD ya no sean necesarios, se deben eliminar de acuerdo con las normas aceptadas en la industria (por ejemplo, mediante un programa de borrado seguro que asegure que los datos no se podrán recuperar).

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 2: Proteger los datos almacenados del titular de la tarjeta

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
2.1 El proveedor de software debe asesorar a los clientes sobre cómo eliminar de manera segura los datos del titular de la tarjeta después de que haya caducado el período de retención definido por el cliente. ***Concuerda con el Requisito 3.1 de las PCI DSS***	**2.1** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que la documentación incluya la siguiente guía para los clientes y los integradores/revendedores: • Se deben eliminar 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 del titular de la tarjeta (para que el cliente sepa las ubicaciones de los datos que se deben eliminar). • Instrucciones que los clientes necesitan para eliminar los datos del titular de la tarjeta de modo seguro cuando ya no sean necesarios para fines legales, reglamentarios o comerciales. • Instrucciones sobre cómo eliminar de modo seguro los datos del titular de la tarjeta almacenados por la aplicación de pago, incluidos los datos almacenados en el software o los sistemas subyacentes (como OS, bases de datos, etc.). • 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.	Para cumplir con el Requisito 3.1 de las PCI DSS, el proveedor debe proporcionar los detalles de todas las ubicaciones donde la aplicación de pago puede almacenar datos del titular de la tarjeta, que incluyan todo software o sistema subyacente (como el OS, bases de datos, etc.), así como instrucciones para eliminar de manera segura los datos de estas ubicaciones después de que los datos hayan excedido el período de retención definido por el cliente. También se les deben proporcionar a los clientes y revendedores/integradores los detalles de configuración del software y sistema subyacente en el que se ejecuta la aplicación a fin de garantizar que estos sistemas subyacentes no capturen los datos del titular de la tarjeta sin el conocimiento del cliente. Para poder evitar la captura o para garantizar que los datos estén protegidos adecuadamente, el cliente debe saber cómo los sistemas subyacentes pueden capturar datos de la aplicación.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
2.2 Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN. ***Nota:*** *Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).* ***Concuerda con el Requisito 3.3 de las PCI DSS***	**2.2.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que la documentación incluya la siguiente guía para los clientes y para los integradores/revendedores: • Detalles de todas las instancias en las que se muestra el PAN, que incluyen, entre otras, los dispositivos de POS, las pantallas, los registros y los recibos. • Confirmación de que la aplicación de pago oculta el PAN de manera predeterminada en todas las vistas. • Instrucciones sobre cómo configurar la aplicación de pago de modo que solo el personal con una necesidad comercial legítima pueda ver el PAN (número de cuenta principal) completo.	La presentación de un PAN (número de cuenta principal) completo en pantallas de computadoras, recibos de tarjetas de pago, faxes o informes impresos puede facilitar la obtención y el uso fraudulento de estos datos por parte de personas malintencionadas. El enfoque de ocultamiento siempre deberá garantizar que solo se muestre el número mínimo de dígitos necesario para realizar una función comercial específica. Por ejemplo, si solo se necesitan los últimos cuatro dígitos para realizar una función comercial, enmascare el PAN para que las personas que realizan esa función solo puedan ver los últimos cuatro dígitos.
	2.2.b Instale la aplicación de pago y revise todas las vistas de los datos del PAN (número de cuenta principal), que incluyen, entre otros, los dispositivos, las pantallas, los registros y los recibos de POS (puntos de venta). Para cada instancia donde se muestre el PAN (número de cuenta principal), compruebe que esté oculto cuando se muestre.	A manera de otro ejemplo, si una función necesita tener acceso al número de identificación bancaria (BIN) para fines de enrutamiento, quite el ocultamiento solo de los dígitos del BIN (tradicionalmente los primeros seis dígitos) durante esa función. Este requisito se relaciona con la protección del PAN que se muestra en pantallas, recibos impresos, impresiones etc., y no se debe confundir con el Requisito 2.3 para la protección del PAN cuando se almacena en archivos, bases de datos, etc.
	2.2.c Configure la aplicación de pago de acuerdo a la *Guía de implementación de la PA-DSS* para permitir únicamente al personal con una necesidad comercial legítima que vea más que los primeros seis/cuatro últimos dígitos del PAN. Para cada instancia en la que se muestra el PAN, revise las configuraciones de la aplicación y las visualizaciones de PAN para verificar que las instrucciones para enmascarar el PAN son exactas, y que solo el personal con una necesidad comercial legítima puede ver más que los primeros seis/cuatro últimos dígitos del PAN.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
2.3 Convierta el PAN (número de cuenta principal) en 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: • Valores hash de una vía basados en cifrado sólido (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 administración de claves.	**2.3.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que la documentación incluya la siguiente guía para los clientes y para los integradores/revendedores: • Detalles de cualquier opción que pueda ser configurada para cada método que utiliza la aplicación para hacer que los datos del titular de la tarjeta sean ilegibles, e instrucciones sobre cómo configurar cada método para todas las ubicaciones donde la aplicación de pago almacene datos de los titulares de la tarjeta (de acuerdo con el Requisito 2.1 de las PA-DSS). • Una lista de todas las instancias en que los datos del titular de la tarjeta puedan extraerse de la aplicación de pago para que el cliente los almacene fuera de esta, e instrucciones que el cliente debe seguir para hacer que los PAN sean ilegibles en tales instancias. • La indicación de que si los registros de depuración se activan (por ejemplo, para solucionar problemas), y los registros incluyen el PAN, se deben proteger de conformidad con la PCI DSS, desactivarlos tan pronto como se haya completado la resolución de problemas, y eliminarlos de manera segura cuando ya no sean necesarios.	La ausencia de protección de los PAN puede permitir que personas malintencionadas vean o descarguen estos datos. Las funciones hash de una vía basadas en criptografía sólida se pueden utilizar para convertir los datos del titular de la tarjeta en ilegibles. Las funciones hash son apropiadas cuando no existe necesidad de recuperar el número original (las funciones hash de una vía son irreversibles). El objetivo del truncamiento es que solo se almacene una parte (sin exceder los primeros seis y los últimos cuatro dígitos) del PAN (número de cuenta principal). Un token de índice es un token criptográfico que reemplaza el PAN (número de cuenta principal) basándose en un índice determinado por un valor impredecible. Un ensamblador único es un sistema en el que una clave privada generada aleatoriamente solo se utiliza una única vez para cifrar un mensaje, que luego se descifra utilizando un ensamblador y una clave únicos que coincidan.
Notas: • 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 truncadas del mismo PAN (número de cuenta principal), se deben implementar controles adicionales para garantizar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN (número de cuenta principal) original.	**2.3.b** Revise el método utilizado para proteger el PAN, incluidos los algoritmos de cifrado (si corresponde). Compruebe que el PAN (número de cuenta principal) sea ilegible mediante el uso de uno de los siguientes métodos: • 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 asociados para la administración de claves.	El objetivo de una criptografía sólida (según se define en el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS*) es que el cifrado se base en un algoritmo probado y aceptado por la industria (no, en un algoritmo de propiedad exclusiva ni desarrollado internamente), con claves criptográficas sólidas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
• El PAN se debe convertir en ilegible en todo lugar donde se almacene, incluso fuera de la aplicación de pago (por ejemplo, la salida de archivos de registro de la aplicación para almacenar en el entorno del cliente). ***Concuerda con el Requisito 3.4 de las PCI DSS***	**2.3.c** Si la aplicación crea dos versiones hash y truncadas del mismo PAN, revise los métodos para crear las versiones hash y truncadas para verificar que ellas no pueden correlacionarse para reconstruir el PAN original.	
	2.3.d Revise varias tablas o archivos de los depósitos de datos creados o generados por la aplicación para comprobar que el PAN (número de cuenta principal) sea ilegible.	
	2.3.e 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 extraíbles, revise una muestra de los archivos generados, incluidos los generados en medios extraíbles (por ejemplo, cintas de copias de seguridad), para confirmar que el PAN (número de cuenta principal) sea ilegible.	
	2.3.f 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.	
	2.3.g Si el proveedor de software almacena el PAN (número de cuenta principal) por alguna razón (por ejemplo, porque se recibieron los archivos de registro, de depuración y otras fuentes de datos de parte de los clientes para depurar o resolver problemas), compruebe que el PAN (número de cuenta principal) sea ilegible de acuerdo con los Requisitos del 2.3.b al 2.3.f especificados anteriormente.	
2.4 La aplicación de pago debe proteger las claves utilizadas para garantizar los datos del titular de la tarjeta contra divulgación o uso indebido.	**2.4.a** Revise la documentación del producto y entreviste al personal responsable para comprobar que se implementen los controles que restringen el acceso a las claves criptográficas que utiliza la aplicación.	Las claves criptográficas deben tener una sólida protección debido a que aquellos que obtienen acceso podrán descifrar datos.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
Nota: *Este requisito se aplica a las claves utilizadas para cifrar datos del titular de la tarjeta almacenados y para claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos. Dichas claves de cifrado de claves deben ser tan sólidas como las claves de cifrado de datos, como mínimo.* ***Concuerda con el Requisito 3.5 de las PCI DSS***	**2.4.b** Revise los archivos de configuración de sistemas para controlar lo siguiente: • Las claves se deben almacenar en formato cifrado. • Las claves de cifrado de claves se deben almacenar separadas de las claves de cifrado de datos. • Las claves de cifrado de claves deben ser tan sólidas como las claves de cifrado de datos que protegen, como mínimo. **2.4.c** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que los clientes y los integradores/revendedores reciban la siguiente recomendación: • 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.	El requisito de las aplicaciones de pago para proteger las claves de divulgación y el uso indebido se aplica tanto a claves de cifrado de datos como a claves de cifrado de claves. El objetivo no es cifrar las claves de cifrado de claves; sin embargo, esas claves deben estar protegidas contra la divulgación y el uso indebido, según lo definido en el Requisito 2.4 Muy pocos deben tener acceso a claves de cifrado, usualmente solo aquellos con responsabilidades de custodios.
2.5 La aplicación de pago debe implementar procesos y procedimientos de administración de claves para las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta, incluidos, al menos, los siguientes: ***Concuerda con el Requisito 3.6 de las PCI DSS***	**2.5** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los integradores/revendedores: • Cómo generar, distribuir, proteger, cambiar, almacenar y retirar/reemplazar claves de cifrado, cuando los clientes o integradores/revendedores participen en estas actividades de administración de claves. • Un formulario de Custodio de claves para que los custodios de las claves reconozcan que entienden y aceptan sus responsabilidades.	La manera en la cual se administran las claves criptográficas es una parte crítica de la seguridad continua de la aplicación de pago. Un buen proceso de administración de claves, bien sea manual o automatizado como parte del producto de cifrado, se basa en normas de la industria y abarca todos los elementos clave desde los puntos 2.5.1 hasta 2.5.7. Instruir a los clientes sobre cómo transmitir, almacenar y actualizar claves criptográficas de manera segura ayuda a evitar la divulgación o el uso indebido de las claves a entidades no autorizadas. Este requisito rige para las claves utilizadas para cifrar los datos del titular de la tarjeta almacenados y cualquier clave de cifrado de claves respectiva.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
2.5.1 Generación de claves criptográficas sólidas	**2.5.1.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya instrucciones para que los clientes y los integradores/revendedores generen claves criptográficas de manera segura.	La aplicación de pago debe generar claves sólidas, de conformidad con lo definido en el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS* en "Criptografía sólida".
	2.5.1.b Evalúe la aplicación, incluidos los métodos utilizados para generar claves criptográficas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para generar claves criptográficas sólidas.	
2.5.2 Distribución segura de claves criptográficas	**2.5.2.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya instrucciones para que los clientes y los integradores/revendedores distribuyan claves criptográficas de manera segura.	La aplicación de pago debe distribuir las claves de manera segura, lo que significa que las claves no se distribuyen en texto claro sino que se distribuyen solo mediante procesos autorizados.
	2.5.2.b Evalúe la aplicación, incluidos los métodos utilizados para distribuir claves criptográficas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para distribuir claves criptográficas de manera segura.	
2.5.3 Almacenamiento seguro de claves criptográficas	**2.5.3.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya instrucciones para que los clientes y los integradores/revendedores almacenen claves criptográficas de manera segura.	La aplicación de pago debe almacenar claves de manera segura (por ejemplo, mediante el cifrado con claves de cifrado de claves).
	2.5.3.b Evalúe la aplicación, incluidos los métodos utilizados para almacenar claves criptográficas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para almacenar las claves criptográficas de manera segura.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
2.5.4 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 o después de que cierta cantidad de texto cifrado haya sido producido por una clave determinada), 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*).	**2.5.4.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya las siguientes instrucciones para los clientes y los integradores/revendedores: • Período de cifrado definido para cada tipo de clave utilizado por la aplicación. • Procedimientos para aplicar cambios de clave al final del período de cifrado definido. **2.5.4.b** Evalúe la aplicación, incluidos los métodos para cambiar las claves criptográficas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para aplicar los cambios de clave al final del período de cifrado definido.	Un período de cifrado es el intervalo durante el cual una clave criptográfica particular se puede utilizar para su propósito definido. Las consideraciones para definir el período de cifrado incluyen, pero sin limitarse a, la solidez del algoritmo subyacente, tamaño o longitud de la clave, peligro de riesgo de la clave y la confidencialidad de los datos cifrados. Es imperativo cambiar periódicamente las claves de cifrado cuando han llegado al final de su período de cifrado a fin de minimizar el riesgo de que alguien obtenga las claves de cifrado y las use para descifrar datos.
2.5.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción 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 un componente de la clave en texto claro, etc.) o se sospeche que las claves están en riesgo. ***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.*	**2.5.5.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya la siguiente información para los clientes y los integradores/revendedores: • Instrucciones que indiquen que las claves se deben retirar o reemplazar cuando se haya debilitado su integridad o cuando se sepa o se sospeche que están en riesgo. • Procedimientos para retirar o reemplazar claves (por ejemplo, mediante archivo, destrucción o revocación según corresponda). • Procedimientos para garantizar que las claves retiradas o reemplazadas no se utilicen para operaciones de cifrado.	Las claves que ya no se utilicen, no se necesiten o que se sepa o se sospeche que estén en riesgo se deben eliminar y destruir para garantizar que ya no se puedan utilizar. Si es necesario guardar esas claves (por ejemplo, para respaldar datos cifrados archivados), deben tener una protección segura. La aplicación de pago debe proporcionar y facilitar un proceso para reemplazar claves que deben ser reemplazadas o aquellas que se sepa o se sospeche que estén en riesgo.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	2.5.5.b Evalúe la aplicación, incluidos los métodos utilizados para retirar o reemplazar claves criptográficas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para retirar o reemplazar claves (por ejemplo, mediante archivo, destrucción o revocación, según corresponda).	
	2.5.5.c Evalúe la aplicación con las claves retiradas/reemplazadas para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para que la aplicación no utilice claves retiradas o reemplazadas para operaciones de cifrado.	
2.5.6 Si la aplicación de pago admite operaciones manuales de administración de claves criptográficas en texto claro, estas operaciones deben aplicar conocimiento dividido y control doble. ***Nota:*** *Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.*	**2.5.6.a** Revise la *Guía de implementación de las PA-DSS* y compruebe que incluya la siguiente información para los clientes y los integradores/revendedores: • Detalles de las operaciones manuales de administración de claves criptográficas en texto claro que admite la aplicación. • Instrucciones para aplicar el conocimiento dividido y el control doble en dichas operaciones.	El conocimiento dividido y el control doble de claves se utilizan para eliminar la posibilidad de que una persona tenga acceso a toda la clave. Este control se implementa en las operaciones manuales de administración de claves. El conocimiento dividido es un método por el cual dos o más personas separadas poseen componentes de una clave, pero que, de forma individual, no pueden descifrar la clave criptográfica original. Cada persona conoce su propio componente de la clave, pero no se puede descifrar la clave criptográfica original a partir de cada componente individual. El control doble requiere de dos o más personas para realizar una función, y ninguna de las personas puede usar el material de autenticación de otra ni acceder a este.
	2.5.6.b Evalúe la aplicación, incluidas todas las operaciones manuales de administración de claves criptográficas en texto claro, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* proporcionen el conocimiento dividido y el control doble de las claves necesarios para todos los procedimientos manuales de administración de claves en texto claro.	
2.5.7 Prevención de sustitución no autorizada de claves criptográficas	**2.5.7.a** Revise la *Guía de implementación de las PA-DSS* y controle que incluya instrucciones para que los clientes y los integradores/revendedores impidan la sustitución no autorizada de claves criptográficas.	La aplicación de pago debe definir métodos para que los usuarios de la aplicación se aseguren de que solo se lleven a cabo sustituciones autorizadas de las claves. La

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	2.5.7.b Evalúe la aplicación, incluidos todos los métodos de sustitución de claves, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* impidan la sustitución no autorizada de claves criptográficas.	configuración de la aplicación no debe permitir ni aceptar la sustitución de claves por parte de fuentes no autorizadas o procesos inesperados.
2.6 Proporcione un mecanismo para que no se pueda recuperar ningún material de claves criptográficas o criptograma almacenado por 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. ***Nota:*** *Este requisito solo se aplica si la aplicación de pago utiliza (o si las versiones anteriores de la aplicación de pago utilizaban) materiales de claves criptográficas o criptogramas para cifrar datos del titular de la tarjeta.* ***Concuerda con el Requisito 3.6 de las PCI DSS***	**2.6.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los integradores/revendedores: • Procedimientos que detallen cómo usar las herramientas o los procedimientos suministrados con la aplicación para hacer que el material criptográfico sea irrecuperable. • Cuando las claves ya no se utilicen, los materiales de claves criptográficas se deben convertir en irrecuperables de acuerdo con los requisitos de administración de claves de las PCI DSS. • Procedimientos para volver a cifrar datos históricos con claves nuevas, incluidos los procedimientos para mantener la seguridad de los datos en texto claro durante los procesos de descifrado y recifrado.	Los proveedores deben proporcionar un mecanismo para que los clientes puedan eliminar el material criptográfico anterior cuando el cliente ya no lo necesite. Tenga en cuenta que el material criptográfico anterior se debe eliminar cuando el cliente lo desee. La recuperación de materiales de claves criptográficas y/o criptogramas se puede impedir utilizando herramientas o procesos que incluyen, entre otros: • 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. • 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.
	2.6.b Examine el producto de la aplicación final para controlar que el proveedor proporcione una herramienta o un procedimiento con la aplicación para convertir el material criptográfico en irrecuperable.	
	2.6.c Evalúe la aplicación, incluidos los métodos suministrados para lograr que el material de claves criptográficas sea irrecuperable. Compruebe, mediante el uso de herramientas o métodos forenses, que la herramienta o el procedimiento de borrado seguro suministrado por el proveedor convierta el material criptográfico en irrecuperable, de acuerdo con las normas aceptadas en la industria.	
	2.6.d Evalúe los métodos para volver a cifrar datos históricos con claves nuevas, para comprobar que las instrucciones que figuran en la *Guía de implementación de las PA-DSS* sean útiles para volver a cifrar datos históricos con claves nuevas.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 3: Proporcione funciones de autenticación segura

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
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. En todas las cuentas generadas o administradas por la aplicación, se debe implementar la autenticación segura al concluir la instalación y para cambios subsiguientes después de la instalación. La aplicación debe cumplir los requisitos 3.1.1 hasta 3.1.11, que se describen a continuación: ***Nota:*** *El término "cambios subsiguientes", según se utiliza en el Requisito 3, hace referencia a cualquier cambio en la aplicación que ocasione que las cuentas de usuario regresen a la configuración predeterminada, cambios en la configuración actual de las cuentas y cambios que generen nuevas cuentas o que vuelvan a crear cuentas ya existentes.* ***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.* *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.* ***Concuerda con los Requisitos 8.1 y 8.2 de las PCI DSS***	**3.1.a** Controle la *Guía de implementación de las PA-DSS* creada por el proveedor para comprobar que los clientes y los integradores/revendedores reciban la siguiente información: • Instrucciones claras y precisas sobre cómo la aplicación de pago implementa una autenticación sólida para todas las credenciales de autenticación que la aplicación genera o administra por uno de estos medios: - Implementación de cambios seguros a las credenciales de autenticación al concluir la instalación de acuerdo con los Requisitos 3.1.1 hasta 3.1.11. - Implementación de cambios seguros para cualquier cambio subsiguiente (después de la instalación) a las credenciales de autenticación de acuerdo con los Requisitos 3.1.1 hasta 3.1.11. • Recomendación en la que se sugiera que, para mantener el cumplimiento de las PCI DSS, se debe verificar que los cambios implementados en las configuraciones de autenticación proporcionen métodos de autenticación que sean tan estrictos como los requisitos de las PCI DSS. • Se debe asignar una autenticación segura a todas las cuentas predeterminadas en el entorno. • Recomendación de asignar autenticación segura a cualquier cuenta predeterminada (aún cuando no se utilice) y, luego, desactivar las cuentas o no utilizarlas. • Instrucciones claras y precisas para todas las credenciales de autenticación que utilice la aplicación de pago (pero que no genere ni administre la aplicación) 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 3.1.11, que se describen a continuación, para todos los niveles de la aplicación y las cuentas de usuario con acceso administrativo y para todas las cuentas con acceso a datos del titular de la tarjeta. • Identificación de todas las funciones y las cuentas predeterminadas dentro de la aplicación con acceso administrativo.	Si se asegura que, en la aplicación, cada usuario tenga una identificación única (en lugar de usar una misma ID para varios empleados), se deben implementar los requisitos de las PCI DSS a la aplicación para mantener la responsabilidad individual de las acciones y una pista de auditorías efectiva por empleado. Esto resulta útil para acelerar la resolución de problemas y la contención cuando se producen usos indebidos o acciones malintencionadas. Una autenticación segura, cuando se usa además de las ID exclusivas, ayuda a impedir que las ID de los usuarios corran riesgos, ya que quien intenta poner en peligro una cuenta necesita conocer la ID exclusiva y la contraseña (u otro elemento de autenticación).

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.1.1 La aplicación de pago no utiliza (ni requiere 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). ***Concuerda con el Requisito 2.1 de las PCI DSS***	**3.1.1** Instale y configure la aplicación de pago de acuerdo con la *Guía de implementación de las PA-DSS,* incluida la configuración de cualquier cuenta administrativa para todo el software necesario. Evalúe la aplicación de pago para comprobar que no utilice (ni requiera el uso de) cuentas administrativas predeterminadas para el software necesario.	Las cuentas administrativas predeterminadas (y las contraseñas) son de conocimiento público y conocidas por cualquier persona que conozca la aplicación de pago o los componentes del sistema subyacente. Si se utilizan cuentas administrativas predeterminadas o contraseñas, una persona no autorizada puede obtener acceso a la aplicación y a los datos con solo registrarse con las credenciales conocidas públicamente.
3.1.2 La aplicación debe implementar el cambio de todas las contraseñas predeterminadas de la aplicación para todas las cuentas generadas o administradas por la aplicación al concluir la instalación y para los cambios subsiguientes después de la instalación. Esto se aplica a todas las cuentas, incluidas las cuentas de usuario, aplicación o servicio, y cuentas que utilice el proveedor para proporcionar soporte. ***Nota:*** *Este requisito no se puede cumplir mediante la especificación de un proceso de usuario ni de las instrucciones de la Guía de implementación de las PA-DSS. Al concluir la instalación y los cambios subsiguientes, la aplicación debe impedir técnicamente que las cuentas predeterminadas o integradas se utilicen hasta que no se cambie la contraseña predeterminada.* ***Concuerda con el Requisito 2.1 de las PCI DSS***	**3.1.2** En todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera: **3.1.2.a** Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS*, revise las configuraciones de la cuenta y de la contraseña e intente utilizar todas las contraseñas predeterminadas para comprobar que la aplicación solicita el cambio de las contraseñas predeterminadas de la aplicación de pago al concluir del proceso de instalación. **3.1.2.b** Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y de la contraseña e intente utilizar todas las contraseñas predeterminadas para comprobar que la aplicación solicita el cambio de todas las contraseñas predeterminadas al completar el cambio.	Si la aplicación no solicita el cambio de las contraseñas predeterminadas, la aplicación puede quedar expuesta al acceso no autorizado de cualquier persona que conozca los valores predeterminados.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.1.3 La aplicación de pago asigna ID exclusivas para las cuentas de usuario. ***Concuerda con el Requisito 8.1.1 de las PCI DSS***	**3.1.3** En todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Cada vez que se asigna una ID de usuario exclusiva a un usuario, se debe poder realizar un seguimiento de las veces que esta persona accede a la aplicación de pago y las actividades que realiza.
	3.1.3.a Instale la aplicación de pago de acuerdo con la *Guía de implementación de las PA-DSS* e intente crear diferentes cuentas en la aplicación con la misma ID de usuario para comprobar que esta aplicación solo asigna ID de usuario exclusivas al concluir el proceso de instalación.	
	3.1.3.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que se asignen ID de usuario exclusivas a todas las cuentas al completar el cambio.	
3.1.4 La aplicación de pago emplea, al menos, uno de los siguientes métodos para autenticar a todos los usuarios: ▪ 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. ***Concuerda con los Requisitos 8.2 de las PCI DSS***	**3.1.4** En todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Estos métodos de autenticación, cuando se usan además de las ID exclusivas, ayudan a impedir que las ID de los usuarios corran riesgos, ya que quien intenta poner en peligro la cuenta necesita saber la ID exclusiva y la contraseña (u otro elemento de autenticación).
	3.1.4.a Instale la aplicación de pago de acuerdo con la *Guía de implementación de las PA-DSS* y evalúe los métodos de autenticación para comprobar que la aplicación requiera, al menos, uno de los métodos de autenticación definidos para todas las cuentas al concluir el proceso de instalación.	
	3.1.4.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, evalúe los métodos de autenticación para comprobar que la aplicación requiera, al menos, uno de los métodos de autenticación definidos para todas las cuentas al completar el cambio.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.1.5 La aplicación de pago **no** requiere ni utiliza cuentas y contraseñas de grupo, compartidas o genéricas. ***Concuerda con el Requisito 8.5 de las PCI DSS***	**3.1.5** En todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Si varios usuarios comparten las mismas credenciales de autenticación (por ejemplo, cuenta de usuario y contraseña), es imposible asignar responsabilidad por las acciones de una persona o llevar un registro efectivo de ellas, debido a que una acción determinada pudo haber sido ejecutada por cualquier persona con conocimiento de las credenciales de autenticación.
	3.1.5.a Instale la aplicación de pago de acuerdo con la *Guía de implementación de las PA-DSS*, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que, al concluir del proceso de instalación, la aplicación no requiera ni utilice cuentas y contraseñas de grupo, compartidas o genéricas.	
	3.1.5.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación no utilice cuentas y contraseñas de grupo, compartidas o genéricas, ni dependa de ellas, al completar el cambio.	
3.1.6 La aplicación de pago requiere que la contraseña cumpla con los siguientes requisitos: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.	**3.1.6** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Las personas malintencionadas intentarán buscar cuentas sin contraseñas o cuyas contraseñas sean débiles, para poder acceder a una aplicación o a un sistema. Si las contraseñas son cortas o fáciles de adivinar, será relativamente fácil para una persona malintencionada encontrar estas cuentas débiles y comprometer una aplicación o un sistema utilizando una ID de usuario válida. *(continúa en la página siguiente)*
	3.1.6.a Instale la aplicación de pago de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que, al concluir el proceso de instalación, la aplicación solicite una contraseña con la complejidad y la longitud mínimas que se especifican a continuación: • Longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	3.1.6.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que, al completar el cambio, la aplicación solicite una contraseña con la complejidad y la longitud mínimas que se especifican a continuación: • Longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	Este requisito especifica que las contraseñas deben tener una longitud mínima de siete caracteres y que deben contener caracteres numéricos y alfabéticos. Si no puede alcanzar la longitud mínima de caracteres debido a limitaciones técnicas, las entidades pueden utilizar parámetros de "solidez equivalente" para evaluar sus alternativas. La NIST SP 800-63-1 define la "entropía" como "una medida del grado de dificultad para adivinar o determinar una contraseña o una clave". Para obtener más información sobre el valor de la entropía y la solidez equivalente de una contraseña con diferentes formatos mínimos, puede consultar este y otros documentos que analizan la "entropía de la contraseña".
	3.1.6.c Si la aplicación utiliza un conjunto de caracteres mínimos y una longitud de la contraseña diferente, calcule la entropía de la contraseña que requiere la aplicación y compruebe que sea, al menos, equivalente a los parámetros especificados anteriormente (es decir, una solidez mínima de siete caracteres de longitud con caracteres numéricos y alfabéticos combinados).	
3.1.7 La aplicación de pago requiere que se cambien las contraseñas de usuario, al menos, cada 90 días. ***Concuerda con el Requisito 8.2.4 de las PCI DSS***	**3.1.7** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Las contraseñas/frases que se mantienen vigentes durante largos períodos sin cambiarlas proporcionan a las personas malintencionadas más tiempo para descubrirlas.
	3.1.7.a Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que la aplicación solicite que el usuario cambie su contraseña, al menos, cada 90 días al concluir el proceso de instalación.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	3.1.7.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación solicite que el usuario cambie su contraseña, al menos, cada 90 días al completar el cambio.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.1.8 La aplicación de pago mantiene un historial de contraseñas y requiere que una contraseña nueva sea diferente de las cuatro últimas contraseñas utilizadas. ***Concuerda con el Requisito 8.2.5 de las PCI DSS***	**3.1.8** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Si no se conserva el historial de contraseñas, la efectividad del cambio de contraseñas es menor, dado que se puede volver a utilizar una contraseña anterior una y otra vez. Esta medida de no volver a utilizar las contraseñas durante cierto período reduce la posibilidad de que, en el futuro, se utilicen contraseñas que ya hayan sido descifradas o forzadas.
	3.1.8.a Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que, al concluir el proceso de instalación, la aplicación mantenga un historial de contraseñas y que solicite que la nueva contraseña sea diferente de las últimas cuatro utilizadas.	
	3.1.8.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación mantenga un historial de contraseñas y que solicite que la nueva contraseña sea diferente de las últimas cuatro utilizadas al completar el cambio.	
3.1.9 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. ***Concuerda con el Requisito 8.1.6 de las PCI DSS***	**3.1.9** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Sin la implementación de mecanismos de bloqueo de cuentas, un atacante puede intentar adivinar continuamente una contraseña a través de herramientas manuales o automatizadas (por ejemplo, el craqueo de contraseñas), hasta lograr su objetivo y obtener acceso a la cuenta de un usuario.
	3.1.9.a Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que, al concluir del proceso de instalación, la aplicación bloquee las cuentas de usuario después de más de seis intentos de inicio de sesión no válidos.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	3.1.9.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación bloquee las cuentas de usuario después de más de seis intentos de inicio de sesión no válidos al completar el cambio.	
3.1.10 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. ***Concuerda con el Requisito 8.1.7 de las PCI DSS***	**3.1.10** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Si se bloquea una cuenta debido a que una persona ha estado intentando adivinar una contraseña de manera insistente, los controles para retrasar la reactivación de estas cuentas bloqueadas evitan que la persona malintencionada siga adivinando la contraseña (tendrá que detenerse durante un mínimo de 30 minutos hasta que se reactive la contraseña). Además, si es necesario solicitar la reactivación, el administrador puede validar que es el mismo propietario de la cuenta quien solicita la reactivación.
	3.1.10.a Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que, al concluir el proceso de instalación, la aplicación establece la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID de usuario.	
	3.1.10.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación establece la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID de usuario al completar el cambio.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.1.11 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. ***Concuerda con el Requisito 8.1.8 de las PCI DSS***	**3.1.11** Para todas las cuentas generadas o administradas por la aplicación, evalúe la aplicación de la siguiente manera:	Cuando los usuarios dejan sola una sesión abierta con acceso a la aplicación de pago, es posible que otras personas utilicen esa conexión en ausencia del usuario, lo que generaría un acceso a la cuenta no autorizado o un uso indebido de la cuenta.
	3.1.11.a Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de la cuenta para comprobar que, al concluir el proceso de instalación, la aplicación establezca en 15 minutos o menos el tiempo de inactividad para bloquear una sesión.	
	3.1.11.b Evalúe toda la funcionalidad de la aplicación que genere que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales de las cuentas, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de la cuenta y evalúe la funcionalidad de la aplicación para comprobar que la aplicación establezca en 15 minutos o menos el tiempo de inactividad para bloquear una sesión al completar el cambio.	
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 exclusiva de usuario y autenticación segura. ***Concuerda con los Requisitos 8.1 y 8.2 de las PCI DSS***	**3.2** Revise la *Guía de implementación de las PA-DSS* creada por el proveedor para comprobar que se les recomiende a los clientes e integradores/revendedores que controlen el acceso a cualquier computadora, servidor y base de datos que tenga aplicaciones de pago y datos del titular de la tarjeta por medio de una ID exclusiva de usuario y una autenticación segura que cumpla con las PCI DSS.	Si la aplicación se instala en sistemas que no implementan controles de autenticación e identificación sólidos o si se accede a esta a través de estos sistemas, se puede evadir la autenticación sólida que proporciona la aplicación, lo que genera un acceso inseguro.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.3 Asegure todas las contraseñas de la aplicación de pago (incluidas las contraseñas de las cuentas de aplicación y de usuario) durante la transmisión y el almacenamiento. ***Concuerda con el Requisito 8.2.1 de las PCI DSS***	**3.**3 Realice lo siguiente:	Si se almacenan o transmiten contraseñas de la aplicación de pago sin cifrar en la red, una persona malintencionada puede interceptar la contraseña fácilmente, utilizando un "sniffer" o acceder directamente a las contraseñas en archivos donde estén almacenadas y utilizar estos datos hurtados para obtener acceso no autorizado. Concatenar una variable de entrada exclusiva para cada contraseña antes de aplicar el algoritmo hash reduce la efectividad de los ataques por fuerza bruta. Algunos ejemplos de algoritmos criptográficos unidireccionales sólidos aptos para aplicar la función de hash a las contraseñas son PBKDF2 y Bcrypt.
3.3.1 Use criptografía sólida para convertir a todas las contraseñas de la aplicación de pago en ilegibles durante la transmisión.	**3.3.1.a** Revise la documentación del proveedor y las configuraciones de la aplicación para comprobar que utilice criptografía sólida para convertir a todas las contraseñas en ilegibles en todo momento durante la transmisión.	
	3.3.1.b Para todos los tipos de contraseñas de las aplicaciones, revise la transmisión de contraseñas (por ejemplo, registrándose en la aplicación desde otro sistema y autenticando la aplicación en otros sistemas) para comprobar que utilice criptografía sólida para convertir a todas las contraseñas en ilegibles en todo momento durante la transmisión.	
3.3.2 Utilice un algoritmo criptográfico unidireccional sólido basado en normas aprobadas para convertir a todas las contraseñas de la aplicación de pago en ilegibles durante el almacenamiento. Cada contraseña debe tener una variable de entrada exclusiva concatenada con la contraseña antes de aplicar el algoritmo criptográfico. ***Nota:*** *No es necesario que la variable de entrada sea secreta o impredecible.*	**3.3.2.a** Revise la documentación del proveedor y las configuraciones de la aplicación para comprobar lo siguiente**:** • Uso de un algoritmo criptográfico unidireccional sólido basado en normas aprobadas que convierta las contraseñas almacenadas en ilegibles. • Uso de una variable de entrada exclusiva concatenada con cada contraseña antes de aplicar el algoritmo criptográfico.	
	3.3.2.b Para todo tipo de contraseñas de aplicación, identificar todas las ubicaciones en las que la aplicación puede almacenar contraseñas, incluso dentro de la propia aplicación, en los sistemas subyacentes, archivos de registro, configuración del registro, etc. Para todas las ubicaciones y tipos de contraseñas, revise los archivos de contraseñas almacenadas para verificar que las contraseñas son ilegibles usando un fuerte algoritmo criptográfico de una sola vía, con una variable de entrada única en todo momento cuando se almacena.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
3.4 La aplicación de pago debe limitar el acceso a las funciones o los recursos necesarios y aplicar la menor cantidad de privilegios a las cuentas integradas: • De manera predeterminada, todas las cuentas de servicio/aplicaciones solo tienen acceso a aquellas funciones o recursos que necesitan específicamente a los fines de la cuenta de servicios/aplicaciones. • De manera predeterminada, todas las cuentas de servicio/aplicaciones tienen un nivel mínimo de privilegios asignados a cada función o recurso que requiera la cuenta de servicios/aplicaciones. ***Concuerda con el Requisito 7 de las PCI DSS***	**3.4.a** Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y revise las configuraciones de las cuentas integradas para comprobar lo siguiente al concluir el proceso de instalación: • Todas las cuentas de servicio/aplicaciones solo deben tener acceso a aquellas funciones o recursos que necesitan específicamente a los fines de la cuenta de servicios/aplicaciones. • Todas las cuentas de servicio/aplicaciones deben tener un nivel mínimo de privilegios asignados a cada función o recurso que requiera la cuenta de servicios/aplicaciones. **3.4.b** Evalúe todas las funcionalidades de la aplicación que ocasionen cambios en las cuentas integradas, incluidas aquellas que hagan que las cuentas de usuario regresen a las configuraciones predeterminadas, cambios en las configuraciones actuales, la generación de nuevas cuentas y la nueva generación de cuentas ya existentes. Cualquiera sea el tipo de cambio implementado, revise las configuraciones de las cuentas integradas y evalúe la funcionalidad de la aplicación para comprobar lo siguiente al completar el cambio: • Todas las cuentas de servicio/aplicaciones solo deben tener acceso a aquellas funciones o recursos que necesitan específicamente a los fines de la cuenta de servicios/aplicaciones. • Todas las cuentas de servicio/aplicaciones deben tener un nivel mínimo de privilegios asignados a cada función o recurso que requiera la cuenta de servicios/aplicaciones.	Para limitar el acceso a los datos del titular de la tarjeta y a las funciones confidenciales solo a aquellas cuentas que lo necesiten, se deben definir los requisitos y el nivel de privilegio requerido para cada cuenta integrada, de modo que se puedan ejecutar las funciones asignadas, pero que no se otorgue ningún privilegio o acceso adicional innecesario. Asignar la menor cantidad de privilegios ayuda a evitar que los usuarios sin conocimiento suficiente de la aplicación cambien, de modo accidental o incorrecto, la configuración de la aplicación o alteren las configuraciones de seguridad. Asignar la menor cantidad de privilegios también ayuda a reducir el alcance del daño si una persona no autorizada accede a la ID del usuario.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 4: Registre la actividad de la aplicación de pago

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
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 y debe poder vincular todas las actividades con usuarios individuales. ***Concuerda con Requisito 10.1 de las PCI DSS***	**4.1.a** Instale la aplicación de pago. Evalúe la aplicación para comprobar que las pistas de auditoría de la aplicación de pago se activen automáticamente al momento de la instalación.	Resulta crítico que la aplicación de pago disponga de un proceso o mecanismo que vincule a los usuarios con los recursos de la aplicación a los que acceden, que genere registros de auditoría y que proporcione la capacidad de rastrear actividades sospechosas hasta un usuario específico. Para iniciar una investigación, los equipos de investigaciones forenses posteriores al incidente dependen en gran medida de estos registros.
	4.1.b Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que incluya las siguientes instrucciones: • Cómo instalar la aplicación para que los registros estén configurados y activados de manera predeterminada al completar el proceso de instalación. • 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 a continuación, para todas las opciones de registro que el cliente pueda configurar después de la instalación. • Instrucciones de no desactivar los registros, ya que al hacerlo se incumpliría con las PCI DSS. • Cómo establecer los valores de configuración del registro para que cumplan con las PCI DSS para cualquier componente de software de terceros empaquetado o requerido por la aplicación de pago, para todas las opciones de registro que el cliente pueda configurar después de la instalación.	
4.2 La aplicación de pago debe proporcionar pistas de auditoría automatizadas para reconstruir los siguientes eventos: ***Concuerda con el Requisito 10.2 de las PCI DSS***	**4.2** Revise la configuración de los registros de auditoría y la salida de los registros de auditoría para evaluar la aplicación de pago y realice lo siguiente:	El registro de los eventos en los puntos 4.2.1 a 4.2.7 permite que una organización identifique y rastree actividades posiblemente fraudulentas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
4.2.1 Todos los usuarios individuales acceden a los datos del titular de la tarjeta desde la aplicación.	**4.2.1** Compruebe que todas las personas que acceden a los datos del titular de la tarjeta mediante la aplicación de pago estén registradas.	Los individuos malintencionados podrían obtener conocimiento sobre una cuenta de usuario que tenga acceso a datos del titular de la tarjeta a través de la aplicación o podrían crear una cuenta nueva, no autorizada, para acceder a los datos del titular de la tarjeta. Un registro de todos los accesos individuales a los datos de los titulares de tarjetas puede identificar las cuentas que están en riesgo o que han sido mal utilizadas.
4.2.2 Todas las acciones realizadas por un individuo con privilegios administrativos asignados en la aplicación	**4.2.2** Verifique que se registren todas las acciones realizadas por una persona con privilegios administrativos para la aplicación de pago.	Las cuentas que tienen privilegios aumentados, como una cuenta "administrador", tienen el potencial de afectar de manera relevante la seguridad o la funcionalidad operativa de la aplicación. Sin un registro de las actividades realizadas, la organización no puede rastrear los problemas que surjan por errores administrativos o por el uso fraudulento de privilegios hasta encontrar la acción y persona específicas.
4.2.3 Acceso a las pistas de auditoría de la aplicación que sean administradas por la aplicación o estén dentro de ella.	**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.	Los usuarios malintencionados, a menudo, intentan modificar los registros de auditoría para ocultar sus acciones y un registro de acceso permite a una organización realizar un seguimiento de cualquier discrepancia o posible alteración de registros de una cuenta individual.
4.2.4 Intentos de acceso lógico no válidos	**4.2.4** Verifique que se registren los intentos de acceso lógico no válidos.	Los individuos maliciosos frecuentemente realizarán múltiples intentos de acceso a los sistemas que sean su objetivo. Numerosos intentos de inicio de sesión no válidos pueden ser indicios de que un usuario no autorizado intenta utilizar "fuerza bruta" o adivinar una contraseña.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
4.2.5 Uso y cambio de los mecanismos de identificación y autenticación de la aplicación (incluidos, entre otros, la creación de nuevas cuentas, el aumento de privilegios, etc.) y de todos los cambios, adiciones y eliminaciones de las cuentas de la aplicación con privilegios administrativos o de raíz.	**4.2.5** Compruebe el uso y los cambios de los mecanismos de identificación y autenticación de la aplicación (incluidos, entre otros, la creación de nuevas cuentas, el aumento de privilegios, etc.) y todos los cambios, adiciones y eliminaciones realizados en las cuentas de la aplicación con privilegios administrativos o de raíz.	Sin conocer quién tenía una sesión activa al momento de un incidente, es imposible identificar qué cuentas puedan haber sido utilizadas. Adicionalmente, los usuarios maliciosos pueden intentar manipular los controles de autenticación con el propósito de evitarlos o de suplantar la identidad de una cuenta válida. Las actividades que incluyan, entre otras, la creación de nuevas cuentas, la escalación de privilegios o cambios de permisos de acceso pueden indicar el uso no autorizado de los mecanismos de autenticación de un sistema.
4.2.6 Inicialización, detención o pausa de los registros de auditoría de la aplicación	**4.2.6** Compruebe que se registre lo siguiente: • Inicialización de los registros de auditoría de la aplicación. • Detención o pausa de los registros de auditoría de la aplicación.	Desactivar los registros de auditoría (o pausarlos) antes de que se realicen actividades ilícitas es una práctica común de los usuarios malintencionados que desean evitar ser detectados. La inicialización de registros de auditoría podría indicar que la función del registro fue inhabilitada por un usuario para ocultar sus acciones.
4.2.7 Creación y eliminación de objetos en el nivel de sistema dentro de la aplicación o por la aplicación	**4.2.7** Compruebe que se registre la creación y eliminación de objetos en el nivel del sistema dentro de la aplicación o por la aplicación.	Los usuarios malintencionados, a menudo, crean o reemplazan objetos en el nivel del sistema en el sistema objetivo para controlar una función u operación particular en ese sistema. Si se registran los objetos en el nivel de sistema, como tablas de bases de datos o procedimientos almacenados, cuando se crean o se eliminan, será más fácil determinar si dichas modificaciones fueron autorizadas.
4.3 La aplicación de pago debe registrar, al menos, las siguientes entradas de la pista de auditoría para cada evento: ***Concuerda con el Requisito 10.3 de las PCI DSS***	**4.3** Revise la configuración de los registros de auditoría y la salida de los registros de auditoría para evaluar la aplicación de pago y, para cada evento auditable (desde 4.2), realice lo siguiente:	Mediante el registro de los detalles que figuran en 4.3.1 a 4.3.6 para los eventos auditables que contiene el punto 4.2, es posible identificar rápidamente un posible riesgo y, con suficiente, detalle conocer

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
4.3.1 Identificación de usuarios	**4.3.1** Compruebe que la identificación de usuario se incluya en las entradas del registro.	quién, qué, dónde, cuándo y cómo.
4.3.2 Tipo de evento	**4.3.2** Compruebe que el tipo de evento se incluya en las entradas del registro.	
4.3.3 Fecha y hora	**4.3.3** Compruebe 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.	
4.4. La aplicación de pago debe facilitar el registro centralizado. ***Nota:*** *Algunos ejemplos de esta funcionalidad pueden ser los siguientes:* • 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. ***Concuerda con el Requisito 10.5.3 de las PCI DSS***	**4.4.**a Revise la *Guía de implementación de las PA-DSS* creada por el proveedor para comprobar que los clientes y los integradores/revendedores reciban la siguiente información: • Una descripción de cuáles son los mecanismos de registro centralizados admitidos. • Instrucciones y procedimientos para incorporar los registros de la aplicación de pago a un entorno de registro centralizado. **4.4.b** Instale y configure la aplicación de pago según la *Guía de implementación de las PA-DSS* para comprobar que las instrucciones sean precisas y que proporcione la funcionalidad que facilite la capacidad del cliente para integrar los registros a su servidor centralizado de registros.	Sin la protección adecuada de los registros de auditoría, su integridad y exactitud no se pueden garantizar y los registros de auditoría se pueden considerar inútiles como herramienta de investigación después de una situación de riesgo. Incluir los registros de la aplicación de pago a un sistema de registro centralizado le permite al cliente integrar y correlacionar sus registros y asegurar los registros de manera constante en el entorno.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 5: Desarrolle aplicaciones de pago seguras

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.1 El proveedor de software ha definido e implementado un proceso formal para el desarrollo seguro de aplicaciones de pago, que incluye lo siguiente: • Aplicaciones de pago desarrolladas de acuerdo con las PCI DSS y PA-DSS (por ejemplo, registro y autenticación seguros). • Procesos de desarrollo basados en las normas o en las mejores prácticas de la industria. • Seguridad de la información incorporada en todo el ciclo de vida de desarrollo del software. • Desarrollo de las revisiones de seguridad antes del lanzamiento de la aplicación o de la actualización de una aplicación. ***Concuerda con el Requisito 6.3 de las PCI DSS***	**5.1.a** Revise los procesos de desarrollo de software documentados y compruebe que los procesos estén basados en las normas o en las mejores prácticas de la industria.	Si no se incluye la seguridad durante la definición de los requisitos, el diseño, el análisis y las fases de pruebas de desarrollo del software, se pueden introducir vulnerabilidades de seguridad en el código de aplicaciones de forma inadvertida o malintencionada.
	5.1.b Compruebe que los procesos de desarrollo de software documentados incluyan procedimientos para los siguientes procesos: • Incorporación de seguridad de la información en todo el ciclo de vida de desarrollo del software. • Desarrollo de las aplicaciones de pago según los requisitos de las PCI DSS y PA-DSS.	
	5.1.c Compruebe que los procesos de desarrollo de software documentados incluyan lo siguiente: • Revisiones de seguridad definidas antes del lanzamiento de una aplicación o de una actualización de la aplicación. • Procedimientos de revisión de seguridad desarrollados para garantizar el cumplimiento de los objetivos de las PCI DSS y PA-DSS.	
	5.1.d Entreviste a los desarrolladores de software para confirmar que se respeten los procesos documentados de la siguiente manera: • Seguridad de la información incorporada en todo el ciclo de vida de desarrollo del software. • Desarrollo de las aplicaciones de pago según los requisitos de las PCI DSS y PA-DSS. • Revisiones de seguridad desarrolladas en intervalos definidos a lo largo del proceso de desarrollo y antes del lanzamiento para garantizar que se cumplan los objetivos de seguridad, lo que incluye los requisitos de las PCI DSS y de las PA-DSS.	
5.1.1 Los PAN (número de cuenta principal) activos no se utilizan para las pruebas ni para el desarrollo. ***Concuerda con el Requisito 6.4.3 de las PCI***	**5.1.1.a** Revise los procesos de desarrollo de software para comprobar que incluyan procedimientos que aseguren que los PAN (número de cuenta principal) activos no se utilizan para las pruebas ni para el desarrollo.	Las marcas de tarjetas de pago y muchos adquirientes pueden proporcionar números de cuenta adecuados para realizar pruebas en caso de que se necesiten PAN (número de cuenta
	5.1.1.b Observe los procedimientos de pruebas y entreviste	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
DSS	al personal para verificar que los PAN (número de cuenta principal) activos no se utilizan para pruebas ni para el desarrollo.	principal) reales para llevar a cabo pruebas de la funcionalidad del sistema antes del lanzamiento.
	5.1.1.c Revise muestras de datos de pruebas para comprobar que los PAN (número de cuenta principal) activos no se utilizan para pruebas ni para el desarrollo.	
5.1.2 Los datos y las cuentas de prueba son retirados antes de enviar el producto al cliente. ***Concuerda con el Requisito 6.4.4 de las PCI DSS***	**5.1.2.a** Revise los procesos de desarrollo de software para comprobar que incluyan procedimientos que aseguren que los datos y las cuentas de prueba se eliminen antes de que la aplicación de pago se envíe a los clientes.	Los datos y las cuentas de prueba se deben eliminarse de la aplicación antes de que esta se envíe a los clientes, dado que la inclusión de estos puntos puede revelar información sobre construcciones de claves dentro de la aplicación.
	5.1.2.b Observe los procedimientos de pruebas y entreviste al personal para comprobar que los datos y las cuentas de prueba se eliminen antes del envío a los clientes.	
	5.1.2.c Revise el producto final de la aplicación de pago para comprobar que los datos y las cuentas de prueba se eliminen antes del envío a los clientes.	
5.1.3 Las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago son retiradas antes de enviar las aplicaciones de pago a los clientes. ***Concuerda con el Requisito 6.3.1 de las PCI DSS***	**5.1.3.a** Revise los procesos de desarrollo de software para comprobar que incluyan procedimientos que aseguren que las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago se eliminen antes de que la aplicación de pago se envíe a los clientes.	La versión previa al lanzamiento de las cuentas, de las ID de usuario y de las contraseñas personalizadas puede servir de “puerta trasera” para que los desarrolladores u otras personas con conocimiento de estas cuentas obtengan acceso a la aplicación y puedan poner en riesgo la aplicación y los datos del titular de la tarjeta relacionados.
	5.1.3.b Observe los procedimientos de pruebas y entreviste al personal para comprobar que las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago se eliminen antes de enviar la aplicación de pago a los clientes.	
	5.1.3.c Revise el producto final de la aplicación de pago para comprobar que las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago se eliminen antes de enviar la aplicación de pago a los clientes.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.1.4 El código de la aplicación de pago se revisa antes del envío a los clientes después de implementar algún cambio significativo, a fin de identificar posibles vulnerabilidades de la codificación (ya sea mediante procesos manuales o automáticos) para incluir, al menos, lo siguiente: • Individuos que no sean el autor que originó el código e individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura revisan los cambios en los códigos. • 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. • Los resultados documentados de la revisión de códigos incluyen la aprobación de la gerencia, el autor del código, el revisor del código y las correcciones que se implementaron antes del envío. ***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.* ***Concuerda con el Requisito 6.3.2 de las PCI DSS***	**5.1.4.a** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable para comprobar que el proveedor realiza las revisiones de códigos de todos los cambios de código de las aplicaciones significativos (ya sea mediante procesos manuales o automáticos) de la siguiente manera: • Individuos que no sean el autor que originó el código e individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura revisan los cambios en los códigos. • 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. • Los resultados documentados de la revisión de códigos incluyen la aprobación de la gerencia, el autor que originó el código, el revisor del código y qué correcciones se implementaron antes del envío. **5.1.4.b** Revise los resultados de las revisiones de código para obtener una muestra de los cambios implementados en los códigos para comprobar lo siguiente: • Las revisiones de los códigos fueron desarrollados por una persona experta, distinta del autor del código. • Las revisiones de los códigos se desarrollaron de acuerdo con las directrices de codificación segura. • Se implementaron las correcciones pertinentes antes del envío. • La gerencia revisó y aprobó los resultados de las revisiones de los códigos antes del envío.	Las vulnerabilidades de seguridad en códigos de aplicaciones suelen ser blanco de personas malintencionadas para obtener acceso a una red y poner en riesgo los datos del titular de la tarjeta. Se deben utilizar técnicas adecuadas de revisión de códigos para brindar protección contra este tipo de ataques. Las técnicas de revisión de código deben comprobar que se emplearon las mejores prácticas de codificación segura durante el proceso de desarrollo. El proveedor de la aplicación debe incorporar prácticas de codificación seguras en función de las tecnologías particulares utilizadas. Las revisiones deben estar a cargo de una persona experta en esta tecnología y con experiencia en técnicas de revisión de códigos para identificar posibles problemas de codificación. Asignar las revisiones de los códigos a alguien que no sea el desarrollador del código permite que se realice una revisión independiente y objetiva. Corregir los errores de codificación antes de que se lance el código impide que un código defectuoso exponga los entornos de clientes a un posible uso indebido. Es mucho más difícil y costoso corregir un código defectuoso una vez implementado. Incluir la revisión formal y la aprobación final de la gerencia antes del envío garantiza que el código está aprobado y que se ha desarrollado de acuerdo con las políticas y los procedimientos.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.1.5 Implementación de prácticas seguras de control de código fuente para comprobar la integridad del código fuente durante el proceso de desarrollo.	**5.1.5.a** Revise los procedimientos de desarrollo del software escritos y entreviste al personal responsable para comprobar que el proveedor implemente prácticas seguras de control de código fuente a fin de corroborar la integridad del código fuente durante el proceso de desarrollo.	Por medio de las buenas prácticas de control de código fuente, se garantiza que todos los cambios implementados en los códigos sean intencionales y estén autorizados y que solamente los realicen personas cuyas razones sean legítimas. Algunos ejemplos de estas prácticas son los procedimientos de ingreso y salida de códigos con controles de acceso estrictos, y una comparación inmediata antes de actualizar el código para confirmar que la última versión aprobada no haya sufrido cambios (por ejemplo, utilizar una suma de comprobación).
	5.1.5.b Revise los mecanismos e implemente los procedimientos para proteger el código fuente a fin de comprobar que se mantenga la integridad del código fuente durante el proceso de desarrollo.	
5.1.6 Las aplicaciones de pago se desarrollan de acuerdo con las mejores prácticas de la industria sobre técnicas de codificación seguras, como las siguientes: • Desarrollo con la menor cantidad de privilegios para el entorno de la aplicación. • Desarrollo con valores predeterminados a prueba de errores (de manera predeterminada, se niegan todas las ejecuciones, a menos que se especifique en el diseño inicial). • Desarrollo para todas las consideraciones	**5.1.6.a** Revise los procesos de desarrollo de software para comprobar que se definan técnicas de codificación seguras, que incluyan lo siguiente: • Desarrollo con la menor cantidad de privilegios para el entorno de la aplicación. • Desarrollo de valores predeterminados a prueba de errores (de manera predeterminada, se niegan todas las ejecuciones, a menos que se especifique en el diseño inicial). • Desarrollo para todas las consideraciones de punto de acceso, incluidas las variaciones de entrada, como las entradas multicanal a la aplicación.	El desarrollo de aplicaciones con la menor cantidad de privilegios es la manera más efectiva de garantizar que no ingresen suposiciones inseguras a la aplicación. La introducción de valores predeterminados a prueba de errores puede evitar que el atacante obtenga información confidencial sobre una falla de la aplicación que se pueda utilizar para efectuar ataques posteriores. Garantizar que la seguridad se aplique en todos los accesos y entradas de la aplicación reduce la posibilidad de que un canal de entrada

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
de punto de acceso, incluidas las variaciones de entrada, como las entradas multicanal a la aplicación.	**5.1.6.b** Entreviste a los desarrolladores para comprobar que las aplicaciones estén desarrolladas de acuerdo con las mejores prácticas de la industria sobre técnicas de codificación seguras, como las siguientes: • Desarrollo con la menor cantidad de privilegios para el entorno de la aplicación. • Desarrollo con valores predeterminados a prueba de errores (de manera predeterminada, se niegan todas las ejecuciones, a menos que se especifique en el diseño inicial). • Desarrollo para todas las consideraciones de punto de acceso, incluidas las variaciones de entrada, como las entradas multicanal a la aplicación.	pueda quedar expuesto a riesgos. Si estos conceptos no se tienen en cuenta durante el desarrollo del código, es posible que se lance una aplicación insegura y que sea necesario implementar demasiadas correcciones más tarde.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.1.6.1 Las técnicas de codificación incluyen documentación sobre cómo se manipulan los PAN (número de cuenta principal) y los SAD (datos de autenticación confidenciales) en la memoria.	**5.1.6.1.a** Revise las técnicas de codificación para comprobar que incluyan documentación sobre cómo se manipulan los PAN (número de cuenta principal) y los SAD (datos de autenticación confidenciales) en la memoria.	Los atacantes utilizan herramientas maliciosas para capturar datos confidenciales de la memoria. Minimizar la exposición de los PAN (número de cuenta principal) y los SAD (datos de autenticación confidenciales) mientras están en la memoria ayudará a reducir la posibilidad de que usuarios malintencionados puedan capturarlos o de que se guarden en el disco accidentalmente en un archivo de memoria y queden sin protección. Este requisito tiene por objetivo garantizar que se tenga en cuenta cómo se manipulan los PAN (número de cuenta principal) y los SAD (datos de autenticación confidenciales) en la memoria. Entender cuándo, durante cuánto tiempo y en qué tipo de formato se mantienen los datos confidenciales en la memoria ayudará a los proveedores de la aplicación a identificar posibles amenazas en sus aplicaciones y a determinar si se necesitan protecciones adicionales. Si alguna técnica de codificación surge de esta actividad o no dependerá del software particular que se desarrolle y de las tecnologías que se utilicen.
	5.1.6.1.b Entreviste a los desarrolladores para comprobar si tienen en cuenta cómo se manipulan los PAN (número de cuenta principal) y los SAD (datos de autenticación confidenciales) en la memoria durante el proceso de desarrollo de la aplicación.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.1.7 Proporcione capacitación a los desarrolladores de aplicaciones sobre el desarrollo de prácticas seguras, según corresponda de acuerdo con la función que realice el desarrollador en su cargo y la tecnología que utilice, por ejemplo: • Diseño de aplicaciones seguras. • Técnicas de codificación seguras para evitar vulnerabilidades de codificación comunes (por ejemplo, recomendaciones del proveedor, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.). • Administración de datos confidenciales en la memoria. • Revisión de códigos. • Pruebas de seguridad (por ejemplo, técnicas para las pruebas de penetración). • Técnicas de evaluación de riesgos. ***Nota:*** *La capacitación de los desarrolladores de aplicaciones puede estar a cargo de personal de la empresa o de terceros. La capacitación se puede proporcionar, por ejemplo, en el trabajo, con la orientación de un instructor o por computadora.*	**5.1.7a** Compruebe que los procesos de desarrollo de software documentados requieran de la capacitación de los desarrolladores de aplicaciones sobre desarrollo de prácticas seguras, según corresponda de acuerdo con la función que realice el desarrollador en su cargo y la tecnología que utilice. **5.1.7.b** Entreviste a un grupo modelo de desarrolladores para comprobar si son expertos en el desarrollo de prácticas y técnicas de codificación seguras, según corresponda a la tecnología utilizada. **5.1.7.c** Revise los registros de la capacitación para comprobar que todos los desarrolladores de la aplicación reciban capacitación según la función que desempeñan y la tecnología utilizada.	Garantizar que los desarrolladores sean expertos en el desarrollo de prácticas seguras ayudará a reducir la cantidad de vulnerabilidades de seguridad que puedan presentar las prácticas de codificación deficientes. El personal capacitado tiene más posibilidades de identificar posibles problemas de seguridad en el diseño y en la codificación de la aplicación. Las metodologías y plataformas de desarrollo de software cambian frecuentemente al igual que los riesgos y las amenazas a las aplicaciones de software. La capacitación en el desarrollo de prácticas seguras se debe mantener actualizada para ajustarse al desarrollo de nuevas prácticas.
5.1.7.1 Actualice la capacitación según sea necesario para ajustarse al desarrollo de nuevas tecnologías y métodos utilizados.	**5.1.7.1** Revise los materiales de capacitación y entreviste a un grupo modelo de desarrolladores para comprobar que la capacitación se actualice según sea necesario para ajustarse al desarrollo de nuevas tecnologías y métodos utilizados.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.2 Desarrolle todas las aplicaciones de pago para evitar vulnerabilidades de codificación comunes en los procesos de desarrollo de software. ***Nota:*** *Las vulnerabilidades indicadas en los Requisitos 5.2.1 a 5.2.10 de la PA-DSS y 6.5.1 a 6.5.10 de la 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.* ***Concuerda con el Requisito 6.5 de las PCI DSS***	**5.2.** Compruebe que las aplicaciones de pago no sean susceptibles a las vulnerabilidades de codificación comunes realizando pruebas de penetración manuales o automatizadas que específicamente intenten aprovechar cada una de las siguientes situaciones:	La capa de aplicación es de alto riesgo y puede ser el blanco de amenazas internas y externas. Sin la seguridad apropiada, se pueden exponer los datos del titular de la tarjeta y otra información confidencial de la empresa. Los Requisitos 5.2.1 a 5.2.10 son los controles mínimos que se deben implementar. Esta lista incluye las vulnerabilidades de codificación más comunes al momento en que se publicó esta versión de las PA-DSS. En la medida en que cambien las vulnerabilidades de codificación comunes aceptadas por la industria, las prácticas de codificación de los proveedores se deben actualizar para que coincidan.
Nota: *Los Requisitos 5.2.1 a 5.2.6, que se describen a continuación, rigen para todas las aplicaciones de pago (internas o externas):*		
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** Los errores de inyección, en especial, errores de inyección SQL, se corrigen a través de técnicas de codificación como las siguientes: • Validación de la entrada para comprobar que los datos de usuario no puedan modificar el significado de los comandos y las consultas. • Uso de consultas basadas en parámetros.	Los errores de inyección, en especial, los errores de inyección SQL, son métodos comúnmente utilizados para poner en riesgo aplicaciones. La inyección se produce cuando se envían datos suministrados por el usuario a un intérprete como parte de un comando o una consulta. Los datos hostiles del atacante engañan al intérprete para que ejecute comandos accidentales o cambie datos, lo cual expone a los componentes de la aplicación a riesgos de ataques, como desbordamientos de buffer. La aplicación debe validar los datos de entrada antes de procesarlos, por ejemplo, mediante la verificación de todos los caracteres alfabéticos, la combinación de caracteres numéricos y alfabéticos, etc.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.2.2 Desbordamiento de buffer	**5.2.2** Para corregir el desbordamiento de buffer, se utilizan técnicas de codificación como las siguientes: • Validación de límites del buffer. • Truncamiento de cadenas de entrada.	Los desbordamientos de buffer ocurren cuando una aplicación no tiene los límites necesarios para verificar su espacio de buffer. Esto puede ocasionar la información en el buffer se expulse del espacio de memoria del buffer y que entre en el espacio de memoria ejecutable. Cuando esto ocurre, el atacante puede insertar código malicioso al final del buffer y luego introducir ese código en espacio de memoria ejecutable desbordando el buffer. Luego, el código malicioso se ejecuta y, con frecuencia, permite que el atacante acceda, de manera remota, a la aplicación o al sistema infectado.
5.2.3 Almacenamiento criptográfico inseguro	**5.2.3** El almacenamiento criptográfico inseguro se corrige mediante técnicas de codificación que se caracterizan por lo siguiente: • Previenen errores de cifrado. • Utilice claves y algoritmos criptográficos sólidos.	Las aplicaciones que no utilizan apropiadamente funciones criptográficas sólidas para almacenar datos tienen mayor probabilidad de riesgo y de exposición de credenciales de autenticación o de datos del titular de la tarjeta.
5.2.4 Comunicaciones inseguras	**5.2.4** Las comunicaciones inseguras se corrigen mediante técnicas de codificación que autentiquen y cifren correctamente todas las comunicaciones confidenciales.	Las aplicaciones que no cifran adecuadamente el tráfico de red confidencial utilizando cifrado sólido tienen mayor probabilidad de riesgo y de exposición de datos del titular de la tarjeta.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.2.5 Manejo inadecuado de errores	**5.2.5** El manejo inadecuado de errores se corrige mediante técnicas de codificación que no filtran información por medio de mensajes de error (por ejemplo, enviando detalles genéricos del error en lugar de enviar detalles específicos).	Las aplicaciones que filtran información sobre su configuración, trabajos internos o que exponen información privilegiada mediante métodos inadecuados de manejo de errores podrían presentar peligros. Los atacantes utilizan estas debilidades para hurtar datos confidenciales o para poner en peligro todo el sistema. Si una persona malintencionada puede crear errores que una aplicación no puede manejar correctamente, puede obtener información detallada del sistema, puede crear interrupciones por negación de servicios, puede introducir fallas en la seguridad o puede bloquear la aplicación o el sistema. Por ejemplo, el mensaje “la contraseña suministrada es incorrecta” indica al atacante que la ID de usuario suministrada es correcta y que debe centrar sus esfuerzos solo en la contraseña. Utilice mensajes de error más genéricos, como “no se pueden verificar los datos”.
5.2.6 Todas las vulnerabilidades de “alto riesgo” se detallan en el proceso de identificación de vulnerabilidades en el Requisito 7.1 de las PA-DSS.	**5.2.6** Las técnicas de codificación corrigen cualquier vulnerabilidad de “alto riesgo” que pueda afectar la aplicación y se detallan en el Requisito 7.1 de las PA-DSS.	Todas las vulnerabilidades que se determinen mediante el proceso de clasificación de riesgos de vulnerabilidades del proveedor (que se definen en los Requisitos 7.1 de las PA-DSS) que son de “alto riesgo” y que pueden afectar la aplicación se deben identificar y corregir durante el desarrollo de la aplicación.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
Nota: *Los Requisitos 5.2.7 a 5.2.10, que se describen a continuación, rigen para las aplicaciones basadas en la Web y para las interfaces de aplicaciones (internas o externas):*		Las aplicaciones web tienen riesgos de seguridad únicos basados en su arquitectura así como una facilidad relativa y ocurrencia de riesgo.
5.2.7 Lenguaje de comandos entre distintos sitios (XSS)	**5.2.7** Para corregir el XSS (lenguaje de comandos entre distintos sitios), se utilizan técnicas de codificación como las siguientes: • Validación de todos los parámetros antes de la inclusión. • Uso de técnicas de escape sensibles al contexto.	Los errores de XSS (lenguaje de comandos entre distintos sitios) se producen cuando una aplicación toma datos suministrados por el usuario y los envía a un explorador web sin primero validar ni codificar ese contenido. El XSS (lenguaje de comandos entre distintos sitios) permite a los atacantes ejecutar secuencias en el navegador de la víctima, el cual puede apropiarse de las sesiones del usuario, destruir sitios web, introducir gusanos, etc.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.2.8 Control de acceso inapropiado, como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios.	**5.2.8** Para corregir el control de acceso inapropiado, como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, se utilizan técnicas de codificación que incluyen las siguientes características: • Autenticación correcta de usuarios. • Desinfección de entradas. • No exposición de referencias a objetos internos a usuarios. • Interfaces de usuarios que no permitan el acceso a funciones no autorizadas.	Una referencia a un objeto directo ocurre cuando un desarrollador expone una referencia a un objeto de implementación interna, como un archivo, directorio, registro de base de datos o clave, como un parámetro de URL o formulario. Los atacantes pueden manipular esas referencias para acceder a otros objetos sin autorización. Si un atacante puede enumerar y navegar la estructura del directorio de un sitio web (exposición completa de los directorios), podría obtener acceso a información no autorizada, así como un mayor conocimiento de los trabajos del sitio para utilizar de manera indebida posteriormente. Las interfaces de usuarios que permitan el acceso a funciones no autorizadas pueden ocasionar que individuos malintencionados obtengan acceso a credenciales privilegiadas o a datos del titular de la tarjeta. Limitar el acceso a los recursos de datos ayudará a evitar que recursos no autorizados accedan a los datos del titular de la tarjeta.
5.2.9 CSRF (falsificación de solicitudes entre distintos sitios)	**5.2.9** Para corregir la CSRF (falsificación de solicitudes entre distintos sitios), se utilizan técnicas de codificación que aseguran que las aplicaciones no confíen en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente.	Ante un ataque de CSRF (falsificación de solicitudes entre distintos sitios), el explorador de la víctima que inició sesión debe enviar una solicitud previamente autenticada a una aplicación web vulnerable, lo que le permite al atacante realizar operaciones de cambio de estado que la víctima está autorizada a realizar (por ejemplo, actualizar los detalles de la cuenta, realizar compras o, incluso, autenticar la aplicación).

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.2.10 Autenticación y administración de sesión interrumpidas	**5.2.10** Para corregir la autenticación y administración de sesión interrumpidas, se utilizan técnicas de codificación que suelen incluir las siguientes características: • Marcas de tokens de sesión (por ejemplo, cookies) como “seguros”. • No exposición de las ID de la sesión en el URL. • Incorporación de tiempos de espera apropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente.	La autenticación y la administración de sesión seguras impiden que personas malintencionadas pongan en riesgo credenciales, claves o tokens de sesión de cuentas legítimas que, de lo contrario, podrían permitir que un intruso adopte la identidad de un usuario autorizado.
5.3 El proveedor de software debe seguir los procedimientos de control de cambios para todos los cambios que surjan en la aplicación. Los procedimientos de control de cambios deben seguir los mismos procesos de desarrollo de software que los nuevos lanzamientos (según se define en el Requisito 5.1 de las PA-DSS) y deben incluir lo siguiente: ***Concuerda con el requisito 6.4.5 de las PCI DSS***	**5.3.a** Revise los procedimientos de control de cambios del proveedor para ver las modificaciones del software y tome las siguientes medidas: • Compruebe que los procedimientos sigan los procesos de desarrollo de software documentados según se define en el Requisito 5.1. • Compruebe que los procedimientos incluyan los puntos 5.3.1 a 5.3.4 que se describen a continuación. **5.3.b** Entreviste a los desarrolladores para determinar los cambios recientes en la aplicación de pago. Revise los cambios recientes en la aplicación de pago y realice un seguimiento de estos cambios relacionados con la documentación de control de cambios. Para cada cambio revisado, compruebe que se haya documentado lo siguiente de acuerdo con los procedimientos de control de cambios:	Si no se administra adecuadamente, es posible que el impacto de las actualizaciones del software y de los parches de seguridad no se perciba completamente y podría ocasionar consecuencias inesperadas.
5.3.1 Documentación de incidencia	**5.3.1** Compruebe que la documentación que tiene incidencia en el cliente se incluya en la documentación de control de cambios de cada cambio.	Se debe documentar el impacto del cambio para que todas las partes afectadas puedan programar, de manera apropiada, cualquier cambio de procesamiento.
5.3.2 Aprobación de cambio documentada por las partes autorizadas apropiadas	**5.3.2** Compruebe que la aprobación documentada por las partes autorizadas apropiadas esté presente para cada cambio.	La aprobación de las partes autorizadas indica que el cambio es legítimo y que está autorizado por la gerencia.
5.3.3 Pruebas de funcionalidad para comprobar que el cambio no incida de forma adversa en la seguridad del sistema	**5.3.3.a** Para cada cambio de muestra, compruebe que se hayan realizado las pruebas de funcionalidad a fin de verificar que el cambio no incida de forma adversa en la seguridad del sistema.	Se deben llevar a cabo pruebas rigurosas para verificar que la seguridad de la aplicación de pago no se reduce al implementar un cambio. Las pruebas

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	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.	deben validar que todos los controles de seguridad existentes permanezcan implementados, sean reemplazados por controles igualmente sólidos o que sean reforzados después de cualquier cambio a la aplicación.
5.3.4 Procedimientos de detención o desinstalación del producto	**5.3.4** Compruebe que los procedimientos de detención o desinstalación del producto estén preparados para cada cambio.	Para cada cambio, debe haber procedimientos de desinstalación en caso de que el cambio falle o afecte negativamente la seguridad de la aplicación, para permitir que la aplicación vuelva al estado previo.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.4 El proveedor de la aplicación de pago debe documentar y seguir la metodología de control de versiones del software como parte del ciclo de vida de desarrollo del sistema. La metodología debe seguir los procedimientos que se detallan en la *Guía del programa PA-DSS* para los cambios que se implementen en las aplicaciones de pago y debe incluir, al menos, los siguientes aspectos:	**5.4** Revise los procesos de desarrollo de software documentados y compruebe que incluyan la metodología de control de versiones del software del proveedor y que la metodología de control de versiones esté de acuerdo con la Guía del programa PA-DSS. Compruebe que la aplicación de pago siga la metodología de control de versiones, incluidos todos los cambios implementados en la aplicación de pago.	Si no se sigue una metodología de control de versiones bien definida, es posible que los cambios que se implementen en las aplicaciones no estén correctamente definidos y que los clientes y los integradores/revendedores no entiendan el impacto del cambio de versión en la aplicación.
5.4.1 La metodología de control de versiones debe definir los elementos utilizados de las versiones específicas de la siguiente manera: • Información detallada sobre cómo los elementos del esquema de la versión están de acuerdo con los requisitos especificados en la *Guía del programa PA-DSS*. • El formato del esquema de la versión, incluidos el número de elementos, separadores, juego de caracteres, etc. (que comprende caracteres alfabéticos, numéricos y/o alfanuméricos). • Una definición de qué representa cada elemento en el esquema de la versión (p. ej., tipo de cambio, versión principal, secundaria o de mantenimiento, carácter comodín, etc.). • Una definición de los elementos que indican el uso de caracteres comodines. ***Nota:*** *Los caracteres comodines solo se pueden reemplazar por elementos del número de versión que representen cambios que no afecten la seguridad. Consulte el punto 5.4.3 para conocer los requisitos adicionales para utilizar caracteres comodines.*	**5.4.1.a** Revise la metodología de control de versiones documentada para comprobar que incluya lo siguiente: • Información detallada sobre cómo los elementos del esquema de numeración de la versión están de acuerdo con los requisitos especificados en la *Guía del programa PA-DSS.* • Especificación del formato del esquema de numeración de la versión, que incluya la cantidad de elementos, separadores, conjunto de caracteres, etc. (por ejemplo, 1.1.1.N, que se compone de caracteres alfabéticos, numéricos y/o alfanuméricos) • Una definición de qué representa cada elemento en el esquema de numeración de la versión (p. ej., tipo de cambio, versión principal, secundaria o de mantenimiento, carácter comodín, etc.). • Una definición de los elementos que indican el uso de caracteres comodines. **5.4.1.b** Compruebe que los elementos del esquema de versión estén de acuerdo con los tipos de cambios especificados en la Guía del programa PA-DSS. **5.4.1.c** Seleccione una muestra de los cambios recientes en la aplicación de pago, los números de versión asignados y la documentación de control de cambios que especifique el tipo de cambio implementado en la aplicación, y compruebe que los elementos en el número de versión coincidan con los parámetros y los cambios correspondientes, de acuerdo con la metodología de control de versiones documentada.	La metodología de control de versiones del proveedor de la aplicación de pago debe incluir un esquema definido de la versión que identifique, específicamente, los elementos utilizados, el formato de la versión, la jerarquía de los diferentes elementos de la versión, etc., para la aplicación de pago particular. El esquema de la versión debe especificar, claramente, cómo utiliza el número de versión cada uno de los distintos elementos. El esquema de la versión se puede indicar de diferentes maneras, por ejemplo, N.NN.NNA, donde “N” representa un elemento numérico y “A” representa un elemento alfabético. El esquema de control de versiones debe incluir una identificación del conjunto de caracteres (por ejemplo, 0-9, A-Z, etc.) que se pueden utilizar para cada elemento de la versión. Si no hay un esquema de la versión correctamente definido, es posible que el formato del esquema de numeración de la versión no represente con exactitud los cambios implementados en la aplicación.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	5.4.1.d Entreviste a un grupo modelo de desarrolladores y compruebe que sean expertos en el esquema de la versión, incluido el uso aceptable de caracteres comodines en el número de versión.	
5.4.2 La metodología del control de versiones debe indicar el tipo y el impacto de todos los cambios en la aplicación, de acuerdo con la *Guía del programa PA-DSS,* que incluya la siguiente información: • Descripción de todos los tipos de cambio y el impacto de estos en la aplicación. • Definición e identificación específica de los cambios que cumplan estos requisitos: - No tengan impacto sobre la funcionalidad de la aplicación o sus dependencias. - Tengan impacto sobre la funcionalidad de la aplicación pero no tengan impacto sobre la seguridad o los requisitos de las PA-DSS. - No tengan impacto sobre las funciones de seguridad ni los requisitos de las PA-DSS. • Cómo se vincula cada tipo de cambio con un número de versión específico.	**5.4.2.a** Revise la metodología de control de versiones documentada del proveedor de software para comprobar que la metodología del control de versiones incluya los siguientes aspectos: • Descripción de todos los tipos de cambio y el impacto de estos en la aplicación (por ejemplo, los cambios que tengan un impacto alto, bajo o nulo sobre la aplicación). • Definición e identificación específica de los cambios que cumplan estos requisitos: - No tengan impacto sobre la funcionalidad de la aplicación o sus dependencias. - Tengan impacto sobre la funcionalidad de la aplicación pero no tengan impacto sobre la seguridad o los requisitos de las PA-DSS. - No tengan impacto sobre las funciones de seguridad ni los requisitos de las PA-DSS. • Cómo se vincula cada tipo de cambio con un número de versión específico.	
	5.4.2.b Compruebe que la metodología del control de versiones cumpla con los requisitos de la *Guía del programa PA-DSS*.	
	5.4.2.c Entreviste al personal y observe los procesos para cada tipo de cambio para comprobar que se siga la metodología documentada para todos los tipos de cambios.	
	5.4.2.d Seleccione una muestra de los cambios implementados recientemente en la aplicación de pago y revise la documentación del control de cambios que especifique el tipo de cambio implementado en la aplicación, para comprobar que la versión asignada al cambio corresponda al tipo de cambio, de acuerdo con la metodología documentada.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.4.3 La metodología de control de versiones debe identificar específicamente si se utilizan caracteres comodines y, en tal caso, cómo se utilizan. Deben incluirse los siguientes aspectos: • Detalles sobre cómo se utilizan los caracteres comodines en la metodología de control de versiones. • Nunca se utilizan caracteres comodines en cambios que afecten la seguridad o alguno de los requisitos de las PA-DSS. • Nunca se debe utilizar un elemento del número de versión que represente un cambio que no afecte la seguridad (incluido un elemento comodín) para representar un cambio que afecte la seguridad. • Los elementos comodines no deben anticipar elementos de versión que puedan representar cambios que afecten la seguridad. No se deben utilizar elementos de versión que aparezcan después de un elemento comodín para representar cambios que afecten la seguridad. ***Nota:*** *Los caracteres comodines solo se deben utilizar de acuerdo con la Guía del programa PA-DSS.*	**5.4.3.a** Revise la metodología de control de versiones documentada del proveedor de software para comprobar que proporcione identificación específica de cómo se utilizan los caracteres comodines, y que incluya los siguientes aspectos: • Detalles sobre cómo se utilizan los caracteres comodines en la metodología de control de versiones. • Nunca se utilizan caracteres comodines en cambios que afecten la seguridad o alguno de los requisitos de las PA-DSS. • Nunca se debe utilizar un elemento del número de versión que represente un cambio que no afecte la seguridad (incluido un elemento comodín) para representar un cambio que afecte la seguridad. • No se puede utilizar ningún elemento que aparezca a la derecha de un carácter comodín para implementar un cambio que afecte la seguridad. Los elementos de la versión que reflejan un cambio que afecta a la seguridad deben aparecer "a la izquierda" del primer elemento comodín.	El elemento “comodín” de las PA-DSS se puede utilizar, opcionalmente, en el esquema de la versión para representar varios cambios que no afecten la seguridad. Un elemento comodín es el único elemento variable del esquema de la versión del proveedor y se utiliza para indicar que los cambios representados por el elemento comodín son secundarios y no afectan la seguridad entre cada versión. Por ejemplo, un número de versión de 1.1.x puede cubrir las versiones específicas 1.1.2 y 1.1.3, etc., lo que le permite al cliente saber que el código base entre ellos se mantiene inalterable, excepto por algunos tipos de cambios secundarios o superficiales. Cualquier uso de los caracteres comodines se debe definir previamente en la metodología del control de versiones del proveedor y solo se debe utilizar de acuerdo con la *Guía del programa PA-DSS*. ***Nota:*** *El uso de un carácter comodín es opcional y no es necesario.*
	5.4.3.b Compruebe que cualquier uso de los caracteres comodines cumpla con los requisitos de la *Guía del programa PA-DSS*. Por ejemplo, los elementos que aparecen después de un elemento comodín no se pueden utilizar para implementar un cambio que afecte la seguridad.	
	5.4.3.c Entreviste al personal y observe los procesos para cada tipo de cambio para comprobar lo siguiente: • Nunca se utilizan caracteres comodines en cambios que afecten la seguridad o alguno de los requisitos de las PA-DSS. • No se deben utilizar elementos del número de versión que representen un cambio que no afecte la seguridad (incluido un elemento comodín) para representar un cambio que afecte la seguridad.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	5.4.3.d Seleccione una muestra de los cambios implementados recientemente en la aplicación de pago y revise la documentación de control de cambios que especifique el tipo de cambio en la aplicación. Compruebe lo siguiente: • Nunca se deben utilizar caracteres comodines en cambios que afecten la seguridad o alguno de los requisitos de las PA-DSS. • No se deben utilizar elementos del número de versión que representen cambios que no afecten la seguridad (incluido un elemento comodín) para representar un cambio que afecte la seguridad.	
5.4.4 La metodología de control de versiones publicada del proveedor se debe informar a los clientes y a los integradores/revendedores.	**5.4.4** Compruebe que la *Guía de implementación de las PA-DSS* incluya una descripción de la metodología de control de versiones publicada del proveedor para los clientes y los integradores/revendedores, y que incluya lo siguiente: • Información detallada sobre el esquema de control de versiones, que incluya el formato del esquema de la versión (cantidad de elementos, separadores, conjunto de caracteres, etc.). • Información detallada sobre cómo se indicarán los cambios que afectan la seguridad en el esquema de la versión. • Información detallada sobre cómo afectarán la versión otros tipos de cambios. • Información detallada sobre los elementos comodines que se utilizan, que incluya una confirmación de que nunca se utilizarán para representar un cambio que afecte la seguridad.	Asegurar que se incluya la metodología de control de versiones del proveedor en la *Guía de implementación de las PA-DSS* proporcionará a los clientes y a los integradores/revendedores la información necesaria para entender qué versión de la aplicación de pago están utilizando y los tipos de cambios que se han implementado en cada versión de la aplicación de pago.
5.4.5 Si se utiliza una versión interna para asignar un esquema de control de versiones publicado, la metodología de control de versiones debe incluir una asignación de las	**5.4.5.a** Revise la metodología de control de versiones documentada para comprobar que incluya una asignación de las versiones internas a las versiones externas publicadas.	Algunos proveedores de aplicaciones de pago cuentan con metodologías de control de versiones para uso interno o como referencia que difieren de la

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
versiones internas a las versiones externas.	**5.4.5.b** Revise los cambios recientes para confirmar que la asignación de las versiones internas al esquema de control de versiones publicado está actualizado y coincida con el tipo de cambio, como está definido en la metodología documentada.	metodología de control de versiones que se utiliza para envíos externos (o públicos). En estas situaciones, resulta importante que ambas metodologías de control de versiones estén bien definidas y documentadas, y que la relación entre ambas esté completamente documentada.
5.4.6 El proveedor de software debe implementar un proceso para revisar las actualizaciones de la aplicación de acuerdo con la metodología de control de versiones antes del lanzamiento.	**5.4.6.a** Revise los procesos de desarrollo de software documentados y la metodología de control de versiones para comprobar que se implemente un proceso para controlar que las actualizaciones de la aplicación se realicen de acuerdo con la metodología de control de versiones antes del lanzamiento.	Es fundamental que los proveedores de la aplicación de pago implementen un proceso para asegurar que las actualizaciones de los productos coincidan con el objetivo y el alcance del lanzamiento planificado, y que dichos cambios se comuniquen a los clientes con exactitud. De lo contrario, es posible que se implementen cambios en la aplicación que afecten negativamente la seguridad de la aplicación de los clientes sin que ellos lo sepan.
	5.4.6.b Entreviste a los desarrolladores de software y observe los procesos para comprobar que se revisen las actualizaciones de la aplicación a fin de corroborar que se realicen de acuerdo con la metodología de control de versiones antes del lanzamiento.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.5 Las técnicas de evaluación de riesgos (por ejemplo, el modelo de riesgos de la aplicación) se utilizan para identificar posibles vulnerabilidades y errores en el diseño de seguridad de la aplicación durante el proceso de desarrollo de software. Algunos de los procesos de evaluación de riesgos son los siguientes: • Cobertura de todas las funciones de la aplicación de pago, incluidas, entre otras, las características que afectan la seguridad y aquellas que superan los límites de confianza. • Evaluación de los puntos de decisión de la aplicación, de los flujos de procesos, flujos de datos, almacenamiento de datos y límites de confianza. • Identificación de todas las áreas de la aplicación de pago que interactúan con el PAN (número de cuenta principal), el SAD (datos de autenticación confidenciales) o con el CDE (entorno de datos del titular de la tarjeta), así como cualquier resultado orientado al proceso que pudiera poner en riesgo los datos del titular de la tarjeta. • Una lista de las posibles vulnerabilidades y amenazas que pudieran surgir del análisis de flujo de datos del titular de la tarjeta y de la clasificación de riesgo (por ejemplo, prioridad alta, media o baja) de cada uno. • Implementación de correcciones y medidas preventivas adecuadas durante el proceso de desarrollo. • Documentación de la evaluación de riesgos para la revisión y el análisis de la gerencia.	**5.5** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable para comprobar que el proveedor utiliza técnicas de evaluación de riesgos como parte del proceso de desarrollo de software y que dicho proceso incluya los siguientes puntos: • Cobertura de todas las funciones de la aplicación de pago, incluidas, entre otras, las características que afectan la seguridad y aquellas que superan los límites de confianza. • Evaluación de los puntos de decisión de la aplicación, de los flujos de procesos, flujos de datos, almacenamiento de datos y límites de confianza. • Identificación de todas las áreas de las aplicaciones de pago que interactúan con el PAN (número de cuenta principal), el SAD (datos de autenticación confidenciales) o con el CDE (entorno de datos del titular de la tarjeta), así como cualquier resultado orientado al proceso que pudiera poner en riesgo los datos del titular de la tarjeta. • Una lista de las posibles vulnerabilidades y amenazas que pudieran surgir del análisis de flujo de los datos del titular de la tarjeta y de la clasificación de riesgo (por ejemplo, prioridad alta, media o baja) de cada uno. • Implementación de correcciones y medidas preventivas adecuadas durante el proceso de desarrollo. • Documentación de la evaluación de riesgos para la revisión y el análisis de la gerencia.	Para mantener la calidad y la seguridad de las aplicaciones de pago, los proveedores de la aplicación deben emplear técnicas de evaluación de riesgos durante el proceso de desarrollo de software. El modelo de riesgos constituye una forma de evaluación de riesgos que se puede utilizar para analizar las construcciones de la aplicación y el flujo de datos en oportunidades en las que usuarios no autorizados de la aplicación pudieran poner en riesgo la información confidencial. Estos procesos les permiten a los desarrolladores y a los arquitectos de software identificar y resolver posibles problemas de seguridad durante el inicio del proceso de desarrollo, lo que mejora la seguridad de la aplicación y reduce los costos de desarrollo.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
5.6 El proveedor de software debe implementar un proceso para documentar y autorizar el lanzamiento final de la aplicación y de cualquier actualización. La documentación debe incluir lo siguiente: • Firma de una parte autorizada que apruebe formalmente el lanzamiento de la aplicación o de su actualización. • Confirmación de que el proveedor siguió los procesos de desarrollo seguro.	**5.6.a** Revise los procesos documentados para comprobar que el lanzamiento final de la aplicación y de cualquier actualización estén formalmente aprobados y documentados, y que incluyan la firma de una parte autorizada que apruebe formalmente el lanzamiento y la confirmación de que se siguieron todos los procesos del SDLC (ciclo de vida de desarrollo del software).	Una persona dentro de la organización del proveedor de la aplicación de pago debe ser responsable de revisar y asegurar que se hayan cumplido todos los aspectos del proceso de desarrollo seguro (según se define en los Requisitos 5.1 a 5.5). Si no se realiza una revisión formal, con la correspondiente aprobación de una parte responsable, se podrían descuidar u omitir procesos de seguridad críticos, lo que provocaría fallas en la aplicación o reduciría su seguridad.
	5.6.b Para obtener una muestra de los lanzamientos y de las actualizaciones de la aplicación recientes, revise la documentación de la aprobación y compruebe que incluya lo siguiente: • La aprobación formal y la firma de una parte autorizada. • Confirmación de que se siguieron todos los procesos de desarrollo seguro.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 6: Proteja las transmisiones inalámbricas

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
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. ***Concuerda con los Requisitos 1.2.3 y 2.1.1 de las PCI DSS***	**6.1** En cuanto a las aplicaciones de pago desarrolladas para utilizar con tecnología inalámbrica y a todas las aplicaciones inalámbricas combinadas con la aplicación de pago, compruebe que las aplicaciones inalámbricas no utilicen los valores de configuración predeterminados por el proveedor de la siguiente manera: **6.1.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que incluya la siguiente información para los clientes y para los integradores/revendedores: • La aplicación de pago implementa cambios en las claves de cifrado, en las contraseñas y en las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas durante la instalación para todos los componentes inalámbricos controlados por la aplicación. • Procedimientos para cambiar las contraseñas y las claves de cifrado inalámbricas, incluidas las cadenas SNMP, cada vez que una persona que conozca las claves/contraseñas cesa en sus funciones o se traslada a otro cargo en la empresa. • Instrucciones para cambiar las claves de cifrado, las contraseñas y las cadenas comunitarias SNMP predeterminadas de cualquier componente inalámbrico proporcionado por la aplicación pero que esta no controle. • Instrucciones para instalar un firewall entre las redes inalámbricas y los sistemas que almacenen datos del titular de la tarjeta. • Información detallada de todo el tráfico inalámbrico (que incluya información específica de la información de puerto) que utilizaría la función inalámbrica de la aplicación de pago. • Instrucciones para configurar los firewalls para que nieguen o, si el tráfico es necesario para fines comerciales, permitan solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	La explotación de la tecnología inalámbrica constituye un método común para que personas malintencionadas obtengan acceso a la red y a los datos del titular de la tarjeta. Si las redes inalámbricas no se implementan con suficientes configuraciones de seguridad (incluido el cambio de los parámetros predeterminados), los sniffers inalámbricos pueden espiar el tráfico, capturar datos y contraseñas de manera sencilla e ingresar en una red y atacarla fácilmente. Por estos motivos, las aplicaciones de pago no deben requerir el uso de configuraciones inalámbricas inseguras o predeterminadas. Si los firewalls no restringen el acceso de las redes inalámbricas al CDE (entorno de datos del titular de la tarjeta), las personas malintencionadas que obtengan acceso no autorizado a la red inalámbrica se pueden conectar fácilmente al CDE (entorno de datos del titular de la tarjeta) y poner en riesgo la información de las cuentas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	6.1.b Instale la aplicación de acuerdo con la *Guía de implementación de las PA-DSS* y evalúe las configuraciones inalámbricas y de la aplicación para comprobar lo siguiente, para todas las funcionalidades inalámbricas administradas por la aplicación de pago: • Las claves de cifrado predeterminadas se deben cambiar al momento de la instalación. • Las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas en los dispositivos inalámbricos se deben cambiar en el momento de la instalación. • Las contraseñas/frases de contraseña predeterminadas en los puntos de acceso se deben cambiar en el momento de la instalación. • El firmware de los dispositivos inalámbricos se debe actualizar a los efectos de admitir el cifrado sólido para la autenticación y la transmisión en redes inalámbricas. • Otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos se deben cambiar, si corresponde.	
	6.1.c Para cambiar las contraseñas, las frases de contraseña, las claves de cifrado y las cadenas SNMP (protocolo simple de administración de red) inalámbricas en cualquier funcionalidad inalámbrica administrada por la aplicación de pago, siga las instrucciones que aparecen en la *Guía de implementación de las PA-DSS*. Compruebe que las instrucciones que aparecen en la *Guía de implementación de las PA-DSS* sean precisas y útiles para cambiar las contraseñas, las claves de cifrado y las cadenas SNMP (protocolo simple de administración de red) inalámbricas.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	6.1.c Para cambiar las contraseñas, las frases de contraseña, las claves de cifrado y las cadenas SNMP (protocolo simple de administración de red) predeterminadas en cualquier componente inalámbrico proporcionado con la aplicación de pago, pero no administrado por esta, siga las instrucciones que aparecen en la *Guía de implementación de las PA-DSS*. Compruebe que las instrucciones que aparecen en la *Guía de implementación de las PA-DSS* sean precisas y útiles para cambiar las contraseñas, las claves de cifrado y las cadenas SNMP (protocolo simple de administración de red) inalámbricas.	
	6.1.e Instale la aplicación y evalúe las funciones inalámbricas para comprobar que los puertos y el tráfico inalámbrico que utiliza la aplicación estén de acuerdo con aquellas documentadas en la *Guía de implementación de las PA-DSS*.	
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. ***Nota:*** *Se prohíbe el uso de WEP como control de seguridad.* ***Concuerda con el requisito 4.1.1 de las PCI DSS***	**6.2.a** En el caso de aplicaciones de pago desarrolladas para utilizar con tecnología inalámbrica, evalúe toda la funcionalidad inalámbrica para comprobar que la aplicación utilice las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión.	Usuarios maliciosos pueden utilizar herramientas gratis y disponibles a gran escala para espiar comunicaciones inalámbricas. El uso de criptografía sólida ayuda a limitar la divulgación de información confidencial en las redes inalámbricas. La criptografía sólida es necesaria para la autenticación y la transmisión de los datos del titular de la tarjeta a los efectos de impedir que personas malintencionadas accedan a los datos de una red
	6.2.b En el caso de las aplicaciones inalámbricas combinadas con la aplicación de pago, evalúe toda la funcionalidad inalámbrica para comprobar que utilice las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
	6.2.c Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que incluya las siguientes instrucciones para los clientes y para los integradores/revendedores: • Cómo configurar la aplicación para que utilice las mejores prácticas de la industria (por ejemplo, IEEE 802.11.i) a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión. • Cómo configurar todas las aplicaciones inalámbricas combinadas con la aplicación de pago para que utilice las mejores prácticas de la industria, a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión.	inalámbrica o que utilicen las redes inalámbricas para acceder a otros sistemas o a otros datos.
6.3 Proporcione instrucciones para los clientes sobre el uso seguro de tecnología inalámbrica. ***Nota:*** *Este requisito rige para todas las aplicaciones de pago, independientemente de si la aplicación se desarrolló para utilizar con tecnologías inalámbricas.* **Concuerda con los *Requisitos 1.2.3, 2.1.1 y 4.1.1 de las PCI DSS***	**6.3** Consulte la *Guía de implementación de la PA-DSS* preparada por el proveedor para verificar que los clientes y los revendedores/integradores reciban instrucciones sobre las configuraciones inalámbricas en cumplimiento con la PCI DSS, de la siguiente manera: • Instrucciones para cambiar todas las claves de cifrado, las contraseñas y las cadenas comunitarias SNMP predeterminadas al momento de la instalación. • Instrucciones para cambiar las contraseñas, las claves de cifrado y las cadenas SNMP inalámbricas, cada vez que una persona que conozca las claves/contraseñas cesa en sus funciones o se traslada a otro cargo en la empresa. • Instrucciones para instalar un firewall entre las redes inalámbricas y los sistemas que almacenan datos del titular de la tarjeta y para configurar los firewalls para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta. • Instrucciones para utilizar las mejores prácticas de la industria (por ej., IEEE 802.11i) para proporcionar cifrado sólido para la autenticación y la transmisión.	Los proveedores de la aplicación de pago deberán proporcionar instrucciones para que los clientes configuren la aplicación para que admita el uso de tecnologías inalámbricas, incluso si la aplicación no está explícitamente diseñada para utilizar en un entorno inalámbrico. Las redes inalámbricas son muy comunes, y los clientes deben conocer las configuraciones de seguridad inalámbrica comunes que deben implementar para garantizar la seguridad de la aplicación de pago.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 7: Evalúe las aplicaciones de pago para corregir las vulnerabilidades y para mantener las actualizaciones de la aplicación

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
7.1 Los proveedores de software deben establecer un proceso para identificar y corregir las vulnerabilidades, de la siguiente manera: ***Nota:*** *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).* ***Concuerda con el Requisito 6.1 de las PCI DSS***	**7.1.a** Revise la documentación del proceso de administración de vulnerabilidades para comprobar que los procedimientos se definan de la siguiente manera: • Identificar nuevas vulnerabilidades de seguridad utilizando fuentes conocidas para obtener información sobre vulnerabilidades de seguridad. • Asignar una clasificación de riesgos para todas las vulnerabilidades identificadas. • Evaluar las aplicaciones de pago y las actualizaciones para detectar vulnerabilidades antes del lanzamiento. **7.1.b** Compruebe que los procesos para identificar las nuevas vulnerabilidades e implementar correcciones en la aplicación de pago se apliquen en todo el software que provee la aplicación de pago o que la exige (por ejemplo, servidores web, programas y bibliotecas de terceros).	Los proveedores deben mantenerse al día con respecto a las nuevas vulnerabilidades que podrían afectar sus aplicaciones, que incluyen vulnerabilidades en los componentes subyacentes o en los componentes de software empaquetado o requerido por la aplicación. Los proveedores de la aplicación de pago que conozcan las vulnerabilidades de sus propias aplicaciones o de los componentes subyacentes deben ser capaces de resolver dichas vulnerabilidades antes del lanzamiento, o implementar otros mecanismos para reducir la posibilidad de que la vulnerabilidad se pueda utilizar de manera indebida, en caso de que el parche de seguridad de un tercero no esté disponible inmediatamente.
7.1.1 Identifique nuevas vulnerabilidades de seguridad utilizando fuentes conocidas para obtener información sobre vulnerabilidades de seguridad.	**7.1.1** Entreviste al personal responsable y observe los procesos para comprobar que se identifiquen nuevas vulnerabilidades de seguridad: • En la aplicación de pago y en cualquier sistema o software subyacente proporcionado con la aplicación de pago o requerido por esta. • Utilizando fuentes conocidas (como sitios web de proveedores de software o sistemas, NVD de NIST, CVE de MITRE y los sitios web de US-CERT de DHS).	Las fuentes conocidas se deben utilizar para información sobre vulnerabilidades o parches en componente de software de terceros. Las fuentes de información de vulnerabilidades deben ser confiables y, generalmente, incluir sitios web de proveedores, nuevos grupos industriales, listas de correos o fuentes RSS. Algunos ejemplos de fuentes de la industria son la base de datos nacional de vulnerabilidad del NIST, la lista de vulnerabilidades y exposiciones comunes de MITRE y los sitios web del US-CERT del Departamento de Seguridad Nacional de los EE. UU.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
7.1.2 Asigne una clasificación de riesgos para todas las vulnerabilidades identificadas, incluidas las vulnerabilidades relacionadas con un sistema o software subyacente proporcionado con la aplicación de pago o requerido por esta. ***Nota:*** *Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria y en el posible impacto. Por ejemplo, en los criterios para clasificar las vulnerabilidades, se puede tener en cuenta la puntuación base CVSS, la clasificación del proveedor o el impacto en la funcionalidad de la aplicación.* *Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de "alto riesgo" para la aplicación. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar "críticas" si representan una amenaza inminente, un impacto sobre un componente crítico de la aplicación o si generarían un posible riesgo si no se contemplaran.*	**7.1.2** Entreviste al personal responsable y observe los procesos para comprobar que las nuevas vulnerabilidades de seguridad se asignan a una clasificación de riesgos que incluye las vulnerabilidades relacionadas con cualquier sistema o software subyacente proporcionado con la aplicación de pago o requerido por esta.	Después de que el proveedor identifique una vulnerabilidad que pueda afectar a su aplicación, deberá evaluar y clasificar el riesgo que supone dicha vulnerabilidad. Para eso, es necesario un proceso que controle constantemente las fuentes de la industria para obtener información sobre las vulnerabilidades. Clasificar los riesgos (por ejemplo, como "alto", "medio" o "bajo") les permite a los proveedores identificar, priorizar y corregir los puntos de mayor riego (por ejemplo, lanzar los parches de mayor prioridad más rápidamente) y reducir la probabilidad de que aquellas vulnerabilidades que suponen el mayor riesgo para los entornos de clientes se utilicen de manera indebida.
7.1.3 Evalúe las aplicaciones de pago y las actualizaciones para detectar vulnerabilidades antes del lanzamiento.	**7.1.3** Entreviste al personal responsable y observe los procesos para comprobar que se evalúen las aplicaciones de pago para detectar vulnerabilidades antes del lanzamiento.	En el proceso de administración de vulnerabilidades del proveedor de la aplicación de pago, se deben incluir pruebas adecuadas para garantizar que cualquier vulnerabilidad identificada se corrija correctamente antes del lanzamiento. *Algunos ejemplos de métodos de pruebas pueden ser las técnicas para las pruebas de penetración o pruebas de exploración de vulnerabilidades para identificar posibles vulnerabilidades; por ejemplo, mediante la inserción de datos inesperados o incorrectos o la modificación del tamaño en bits de los datos.*

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
7.2 Los proveedores de software deben establecer un proceso para el desarrollo e implementación oportunos de parches y actualizaciones de seguridad.	**7.2** Revise la documentación del proceso para el desarrollo y la distribución de parches y actualizaciones de seguridad para comprobar que el proceso incluya los procedimientos 7.2.1 a 7.2.2:	Cuando se identifica una vulnerabilidad crítica, se deben desarrollar actualizaciones de software para corregir las vulnerabilidades de seguridad y enviarlas a los clientes lo antes posible a fin de reducir el plazo y la posibilidad de que se utilicen las vulnerabilidades de manera indebida.
7.2.1 Los parches y las actualizaciones se distribuyen a los clientes de manera segura a través de una cadena de confianza conocida.	**7.2.1** Entreviste al personal responsable y observe los procesos para comprobar que los parches y las actualizaciones se distribuyen a los clientes de manera segura a través de una cadena de confianza conocida.	Los parches de seguridad se deben distribuir de manera tal que impidan que personas malintencionadas intercepten las actualizaciones en tránsito, las modifiquen y luego las redistribuyan entre clientes que desconocen estas prácticas.
7.2.2 Los parches y las actualizaciones se envían a los clientes de manera tal que mantienen la integridad del código del parche y la actualización.	**7.2.2** Entreviste al personal responsable y observe los procesos para comprobar que los parches y las actualizaciones se envíen a los clientes de manera tal que mantengan la integridad del código del parche y la actualización.	Las actualizaciones de seguridad deben incluir un mecanismo dentro del proceso de actualización para comprobar que el código de actualización no haya sido reemplazado ni alterado. Algunos ejemplos de comprobaciones de integridad son las sumas de comprobación, los certificados con firma digital, entre otros.
	7.2.2.b Entreviste al personal responsable y observe los procesos de actualización de la aplicación para comprobar que se evalúe la integridad de los parches y las actualizaciones en el sistema objetivo antes de la instalación.	
	7.2.2.c Ejecute el proceso de actualización con código arbitrario y determine si el sistema permitirá que se lleve a cabo la actualización para comprobar que se mantenga la integridad del código del parche y la actualización.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
7.2.3 Proporcione instrucciones para los clientes acerca de la instalación segura de parches y actualizaciones.	**7.2.3** Revise la *Guía de implementación de la PA-DSS* preparada por el proveedor para comprobar que incluya la siguiente información para los clientes y para los integradores/revendedores: • Cómo el proveedor comunicará las notificaciones de los nuevos parches y actualizaciones. • Cómo se entregarán los parches y actualizaciones de una manera segura con una cadena de confianza conocida. • Cómo acceder e instalar parches y actualizaciones en una manera que mantenga la integridad del código de parche y de actualización.	Informar a los clientes e integradores/revendedores del proceso que recibir e instalar parches de manera segura ayuda a proteger la integridad del proceso de actualización y a la aplicación.
7.3 Incluya notas de la versión de todas las actualizaciones de la aplicación junto con información detallada sobre la actualización, el impacto de esta y cómo se cambió el número de la versión para reflejar la actualización de la aplicación.	**7.3.a** Revise los procesos para enviar actualizaciones y entreviste al personal para comprobar que se preparen notas de la versión para todas las actualizaciones y que estas incluyan información detallada de la actualización, el impacto de esta y cómo se cambió el número de la versión para reflejar la actualización de la aplicación. **7.3.b** Revise las notas de la versión para obtener una muestra de las actualizaciones de la aplicación y compruebe que estas se proporcionen junto con la actualización.	Las notas de la versión proporcionan información detallada a los clientes sobre las actualizaciones del software, que incluyen información sobre los archivos y la funcionalidad de la aplicación que se cambiaron, así como cualquier característica relacionada con la seguridad que pueda verse afectada. Las notas de la versión también deben indicar cómo afecta un parche o una actualización en particular al número de versión general asociado con el envío del parche.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 8: Facilite la implementación de una red segura

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
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 lo establecido en las PCI DSS. *Por ejemplo, la aplicación de pago no puede interferir en la instalación de parches, en la protección contra malware, las configuraciones de firewall, ni ningún otro dispositivo, aplicación o configuración que se requiera para cumplir con lo establecido en las PCI DSS.* ***Concuerda con los Requisitos 1, 3, 4, 5 y 6 de las PCI DSS***	**8.1.a** Instale la aplicación en un entorno de laboratorio que cumpla con lo establecido en las PCI DSS, de acuerdo con la *Guía de implementación de las PA-DSS.* Evalúe la aplicación de pago para obtener pruebas de que se puede ejecutar en una red que cumpla plenamente con lo establecido en las PCI DSS.	Las aplicaciones de pago se deben diseñar y desarrollar de tal manera que la instalación y la operación de la aplicación no impidan que una organización implemente otros controles requeridos para cumplir con lo establecido en las PCI DSS. Por ejemplo, la aplicación de pago debe poder operar en un entorno que ejecute soluciones de antivirus (por ejemplo, que no requiera que estas soluciones se desactiven ni se desinstalen).
	8.1.b Evalúe la aplicación y los sistemas subyacentes para comprobar que la aplicación de pago no impida el uso de las funciones de las PCI DSS en los sistemas subyacentes ni interfiera con ellas, por ejemplo, la aplicación no inhibe la instalación de parches ni actualizaciones contra malware, ni interfiere en la operación de otras funciones de las PCI DSS.	
8.2 La aplicación de pago solo debe utilizar o requerir el uso de servicios, protocolos, daemons, componentes, software y hardware dependientes necesarios y seguros, incluidos aquellos proporcionados por terceros, para cualquier funcionalidad de la aplicación de pago. *Nota: TLS y SSL temprana no se consideran criptografía sólida. Las aplicaciones de pago no deben usar, o apoyar el uso de SSL y TLS temprana. Las aplicaciones que utilizan o apoyan TLS no deben permitirse recurrir a SSL.* ***Concuerda con el requisito 2.2.3 de la PCI DSS***	**8.2.a** Revise los servicios, protocolos, daemons, componentes, software y hardware dependientes del sistema activados o requeridos por la aplicación de pago. Compruebe que solo los servicios, protocolos, daemons, componentes, software y hardware dependientes necesarios y seguros se encuentren activados por opción predeterminada.	Existen numerosos protocolos necesarios para un negocio (o tener habilitados por opción predeterminada) que, habitualmente, utilizan personas malintencionadas para poner en riesgo una red o un sistema. La aplicación de pago no deberá requerir el uso de un protocolo inseguro, servicio, daemon, etc. Si la aplicación soporta el uso de servicios inseguros, daemons, protocolos o componentes, deben ser seguros de manera predeterminada.
	8.2.b Instale la aplicación y evalúe sus funciones para comprobar que, en caso de admitir el uso de servicios, protocolos, daemons o componentes inseguros, esté configurada de forma segura por opción predeterminada.	
	8.2.c Compruebe que la *Guía de implementación de las PA-DSS* documente todos los protocolos, servicios, componentes, software y hardware dependientes requeridos que sean necesarios para cualquier funcionalidad de la aplicación de pago, incluidos los proporcionados por terceros.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
8.3 La aplicación de pago no debe requerir el uso de servicios o protocolos que impidan la utilización de tecnologías de autenticación de múltiples factores, ni que interfiera en sus operaciones normales. ***Nota:*** *La autenticación de múltiples factores requiere que al menos 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 múltiples factores. Los métodos de autenticación, también denominados factores, son los siguientes:* • 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 ***Concuerda con el Requisito 8.3 de las PCI DSS***	**8.3.a** Revise la funcionalidad de la aplicación de pago para comprobar que no requiera el uso de ningún servicio o protocolo que impida la utilización de tecnologías de autenticación de múltiples factores , ni que interfiera en sus operaciones normales **8.3.b** Identifique los mecanismos de acceso remoto admitidos por la aplicación y compruebe que no impidan la autenticación de múltiples factores.	Las aplicaciones de pago se deben diseñar y desarrollar de tal manera que la instalación y la operación de la aplicación no requieran que una organización utilice servicios o protocolos que le impidan a dicha organización implementar y operar soluciones de autenticación de múltiples factores para el acceso seguro. Por ejemplo, la aplicación no debe utilizar, de manera predeterminada, el puerto 1812 (conocido ampliamente porque RFC 2865 lo asigna a RADIUS) si RADIUS tiene por objetivo ser una tecnología de autorización y autenticación admitida. *Algunos ejemplos de tecnologías de dos factores son, entre otras, RADIUS con tokens, TACACS con tokens u otras tecnologías que faciliten la autenticación de múltiples factores.*

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 9: Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
9.1 La aplicación de pago se debe desarrollar de manera que cualquier servidor web y cualquier componente de almacenamiento de datos del titular de la tarjeta (por ejemplo, un servidor de la base de datos) no tengan que estar en el mismo servidor ni sea necesario que el componente de almacenamiento de datos se encuentre en la misma zona de red (como DMZ) que el servidor web. ***Concuerda con el Requisito 1.3.7 de las PCI DSS***	**9.1.a** Identifique todos los componentes de almacenamiento de datos de la aplicación de pago (por ejemplo, bases de datos) y todos los servidores web. Instale los componentes de almacenamiento de datos y los servidores web en diferentes servidores y evalúe la funcionalidad de la aplicación en diferentes servidores. Compruebe que la aplicación de pago no requiera ningún componente de almacenamiento de datos (como una base de datos) para poder instalarla en el mismo servidor que el servidor web para que funcione.	Cualquier componente del servidor web de la aplicación de pago representa un riesgo considerablemente mayor debido a la naturaleza abierta de las redes públicas (Internet, tecnologías inalámbricas públicas, etc.) y a la naturaleza y al volumen de los ataques que pueden originar estas redes. Los componentes de almacenamiento de datos del titular de la tarjeta requieren de un mayor nivel de protección que los componentes públicos de la aplicación. Si los datos del titular de la tarjeta se encuentran en la DMZ (zona desmilitarizada), un atacante externo puede acceder a esta información con más facilidad porque hay menos capas que
	9.1.b Instale los componentes de almacenamiento de datos y los servidores web en zonas de red diferentes. Evalúe todas las funciones de la aplicación en las zonas de red para comprobar que no sea necesario instalar ningún componente de almacenamiento de datos (como una base de datos) para que la aplicación de pago pueda funcionar en la misma zona de red que el servidor web.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

	9.1.c Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que incluya la siguiente información para los clientes y para los integradores/revendedores: • Instrucciones de no almacenar datos del titular de la tarjeta en sistemas públicos (por ejemplo, el servidor web y el servidor de base de datos no deben estar en el mismo servidor). • Instrucciones sobre cómo configurar la aplicación de pago para utilizar una DMZ (zona desmilitarizada) para separar Internet de los sistemas que almacenan datos del titular de la tarjeta (por ejemplo, instalar un componente del servidor web en una DMZ [zona desmilitarizada] e instalar un componente de almacenamiento de datos en una zona de red interna diferente). • Una lista de los servicios/puertos que necesita utilizar la aplicación para comunicar entre dos zonas de red (para que el cliente pueda configurar sus firewalls para que abran solo los puertos requeridos).	penetrar. Por esta misma razón, los servidores web no se deben almacenar en el mismo servidor que el componente de almacenamiento de datos. Si una persona malintencionada pone en riesgo la cuenta en el servidor web, estaría poniendo en riesgo también la base de datos del titular de la tarjeta sin ningún esfuerzo adicional.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 10: Facilite un acceso remoto seguro a la aplicación de pago

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
10.1 La autenticación de múltiples factores se debe utilizar para todos los accesos remotos a la aplicación de pago que se originen fuera del entorno de clientes. ***Nota:*** *La autenticación de múltiples factores exige utilizar dos de los tres métodos de autenticación (consulte el Requisito 3.1.4 de la PA-DSS para obtener una descripción de los métodos de autenticación).* **Concuerda con el *Requisito 8.3 de las PCI DSS***	**10.1.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que contenga la siguiente información para los clientes y para los integradores/revendedores: • Instrucciones que indiquen que todos los accesos remotos que se originan fuera desde la red del cliente hacia la aplicación de pago deben utilizar la autenticación de múltiples factores para cumplir con los requisitos de la PCI DSS. • Una descripción de los mecanismos de la autenticación de múltiples factores admitidos por la aplicación. • Instrucciones para configurar la aplicación para que admita la autenticación de múltiples factores (dos de los tres métodos de autenticación descritos en el Requisito 3.1.4 de la PA DSS). **10.1.b** Si el proveedor de la aplicación puede acceder remotamente a la aplicación de pago del cliente que se origina fuera del entorno de clientes, revise las políticas del proveedor para comprobar que acepte los requisitos de la autenticación de múltiples factores del cliente en dichos casos.	La autenticación de múltiples factores requiere de dos métodos de autenticación para acceder desde fuera de la red. Los proveedores de la aplicación de pago deberán proporcionar instrucciones a los clientes para que configuren la aplicación de modo tal que permita los dos mecanismos de autenticación de múltiples factores especificados para asegurar que aquellos mecanismos puedan implementarse adecuadamente y cumplan con los requisitos de la PCI DSS. El requisito de la autenticación de múltiples factores se aplica solo cuando el acceso remoto se origina fuera del entorno de clientes.
10.2 Cualquier acceso remoto a la aplicación de pago se debe realizar de forma segura, de la siguiente manera:	**10.2** Compruebe que cualquier acceso remoto se realice de la siguiente manera:	Cualquier mecanismo de acceso remoto empleado por el proveedor de la aplicación de pago o el integrador/revendedor (por

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
10.2.1 Si las actualizaciones de la aplicación de pago se envían mediante acceso remoto a los sistemas de los clientes, los proveedores de software deben informar a los clientes que habiliten las tecnologías de acceso remoto solamente cuando sea necesario para realizar descargas del proveedor y que las deshabiliten inmediatamente después de finalizada la descarga. De manera alternativa, si se entregan por medio de una VPN (red privada virtual) u otra conexión de alta velocidad, los proveedores de software deben sugerirles a sus clientes que configuren correctamente un firewall o un producto firewall personal a fin de garantizar conexiones "siempre activas". ***Concuerda con los Requisitos 1 y 12.3.9 de las PCI DSS***	**10.2.1.a** Si las actualizaciones de la aplicación de pago se envían por medio de un acceso remoto a los sistemas de los clientes, revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que contenga lo siguiente: • Instrucciones para los clientes y los integradores/revendedores sobre cómo utilizar tecnologías de acceso remoto de modo seguro. Se debe especificar que dichas tecnologías utilizadas por los proveedores y socios comerciales se deben activar solo cuando sea necesario y desactivar inmediatamente después de utilizarlas. • Recomendación para los clientes y los integradores/revendedores de que utilicen un firewall o un producto firewall personal en caso de que la computadora esté conectada por una VPN (red privada virtual) u otra conexión de alta velocidad, a fin de garantizar que estas conexiones estén "siempre activas", de acuerdo con el Requisito 1 de las PCI DDS.	ejemplo, para proporcionar servicios de soporte técnico) debe admitir todos los requisitos de las PCI DSS que correspondan.
	10.2.1.b Si el proveedor envía la aplicación de pago o las actualizaciones por medio de un acceso remoto a las redes del cliente, observe los métodos que utiliza el proveedor para enviar la aplicación de pago o las actualizaciones por medio de un acceso remoto a las redes del cliente, y compruebe que estos métodos incluyan lo siguiente: • Activación de las tecnologías de acceso remoto para las redes del cliente solo cuando sea necesario y desactivación inmediata después de su uso. • Si el acceso remoto se realiza por medio de una VPN (red privada virtual) u otra conexión de alta velocidad, la conexión se debe proteger de acuerdo con el Requisito 1 de las PCI DSS.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
10.2.2 Si los proveedores o integradores/revendedores pueden acceder a las aplicaciones de pago de los clientes remotamente, se debe utilizar una credencial de autenticación única (como una contraseña/frase) para cada entorno de cliente. ***Concuerda con el Requisito 8.5.1 de las PCI DSS***	**10.2.2** Si los proveedores o integradores/revendedores pueden acceder a las aplicaciones de pago de los clientes remotamente, revise los procesos del proveedor y entreviste al personal para comprobar que se utilice una contraseña única para cada entorno de cliente al que tengan acceso.	Para evitar poner riesgo los entornos de varios clientes mediante el uso de un solo conjunto de credenciales, los proveedores que tienen cuentas con acceso remoto a los entornos de clientes deben utilizar una credencial de autenticación diferente para cada cliente. Evite utilizar fórmulas repetibles para generar contraseñas que se puedan averiguar fácilmente. Estas credenciales se pueden conocer con el tiempo y personas no autorizadas pueden utilizarlas para poner en riesgo a los clientes del proveedor.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
10.2.3 El acceso remoto de los proveedores, integradores/revendedores o clientes a las aplicaciones de pago de los clientes se debe implementar de modo seguro, por ejemplo: • 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 a 3.1.11 de las PA-DSS). • Activar la transmisión de datos cifrados de acuerdo con el Requisito 12.1 de las PA-DSS. • Activar el bloqueo de la cuenta después de una determinada cantidad de intentos fallidos de inicio de sesión. (Consulte los Requisitos 3.1.9 a 3.1.10 de las PA-DSS). • Establecer una conexión VPN (red privada virtual) a través de un firewall antes de permitir el acceso. • Activar la función de inicio de sesión. • Restringir el acceso a entornos de clientes a personal autorizado de los integradores/revendedores. ***Concuerda con los Requisitos 2; 8 y 10 de las PCI DSS***	**10.2.3.a** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que los clientes y los integradores/revendedores reciban instrucciones para implementar todos los accesos remotos a la aplicación de pago de manera segura, por ejemplo: • 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 a 3.1.11 de las PA-DSS). • Activar la transmisión de datos cifrados de acuerdo con el Requisito 12.1 de las PA-DSS. • Activar el bloqueo de la cuenta después de una determinada cantidad de intentos fallidos de inicio de sesión. (Consulte los Requisitos 3.1.9 a 3.1.10 de la PA-DSS). • Establecer una conexión VPN (red privada virtual) a través de un firewall antes de permitir el acceso. • Activar la función de inicio de sesión. • Restringir el acceso a entornos de clientes al personal autorizado. **10.2.3.b** Si el proveedor del software puede acceder a las aplicaciones de pago del cliente remotamente, observe los métodos de acceso remoto del proveedor y entreviste al personal para comprobar que el acceso remoto se implemente de manera segura.	Los proveedores de la aplicación de pago deberán proporcionar instrucciones a los clientes y a los integradores/revendedores para configurar la aplicación, para permitir el acceso remoto seguro, a fin de garantizar que dichos mecanismos se puedan implementar correctamente y que cumplan con los requisitos de las PCI DSS. Este requisito rige para todos los tipos de acceso remoto utilizados para acceder a entornos de clientes.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 11: Cifre el tráfico sensitivo de las redes públicas

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
11.1 Si la aplicación de pago envía o facilita el envío de datos de titulares de tarjetas mediante redes públicas, la aplicación de pago debe admitir el uso de sólidos protocolos de criptografía y seguridad, como la capa de sockets seguros (SSL), la seguridad de la capa de transporte (TLS) y el protocolo de seguridad de Internet (IPSEC) para proteger los datos confidenciales de titulares de tarjetas durante la transmisión a través de redes públicas abiertas. • Solo se aceptan claves y certificados de confianza. • El protocolo implementado solo admite configuraciones o versiones seguras. • La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. ***Nota:*** *SSL y TLS temprana no se consideran criptografía sólida. Las aplicaciones de pago no deben usar, o apoyar el uso de SSL y TLS temprana. Las aplicaciones que utilizan o soportan TLS no deben permitirse recurrir a SSL* *Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes:* • La Internet • Tecnologías inalámbricas, incluidas la 802.11 y Bluetooth, entre otras	**11.1.a** Si la aplicación de pago envía o facilita el envío de datos del titular de la tarjeta por redes públicas, compruebe que se proporcione criptografía sólida o protocolos de seguridad con la aplicación, o que se especifique cómo utilizarlos. **11.1.b** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que se incluyan instrucciones para los clientes y los integradores/revendedores sobre cómo utilizar la criptografía sólida y los protocolos de seguridad proporcionados con la aplicación o especificados para utilizar con esta, y que se incluyan los siguientes aspectos: • Instrucciones para utilizar criptografía sólida y protocolos de seguridad siempre que los datos del titular de la tarjeta se transmitan a través de redes públicas. • Instrucciones para comprobar que solo se acepten claves o certificados de confianza. • Cómo configurar la aplicación de pago para utilizar solo versiones seguras e implementaciones seguras de los protocolos de seguridad. • Cómo configurar la aplicación de pago para evitar el retroceso a una versión o configuración insegura (por ejemplo, si se utiliza TLS, la aplicación no debe permitirse recurrir a SSL). • Cómo configurar la aplicación de pago para utilizar la solidez de cifrado adecuada según la metodología de cifrado que se utilice.	La información confidencial debe estar cifrada durante la transmisión en redes públicas, ya que es sencillo y común para una persona malintencionada interceptar o desviar datos mientras están en tránsito. Para transmitir datos del titular de la tarjeta de manera segura, es necesario utilizar claves/certificados de confianza, protocolos de transmisión seguros y la solidez de cifrado correcta para cifrar los datos del titular de la tarjeta. Tenga en cuenta que algunas implementaciones de protocolos (como SSL, SSH versión 1.0 y TLS temprana) tienen vulnerabilidades documentadas, como desbordamientos de buffer, que un atacante puede utilizar para obtener el control del sistema afectado. Independientemente de los protocolos de seguridad que utilice la aplicación de pago, asegúrese de que estén configurados de manera predeterminada para utilizar solo configuraciones y versiones seguras y así impedir el uso de una conexión insegura.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
• Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código) • Servicio de radio paquete general (GPRS) • Comunicaciones satelitales ***Concuerda con el Requisito 4.1 de las PCI DSS***	**11.1.c** Si la aplicación de pago incluye criptografía sólida y protocolos de seguridad, instale y evalúe la aplicación de acuerdo con las instrucciones que figuran en la *Guía de implementación de las PA-DSS* y compruebe lo siguiente: • El protocolo se debe implementar de manera predeterminada para utilizar solo claves o certificados de confianza. • El protocolo se debe implementar de manera predeterminada para utilizar solo configuraciones seguras, y no debe admitir versiones o configuraciones inseguras. • El protocolo se implementa de manera predeterminada para no permitir retroceso a una versión o configuración insegura (por ejemplo, si se utiliza TLS, la aplicación no debe permitirse recurrir a SSL). • Se debe implementar la solidez de cifrado correcta según la metodología de cifrado que se utilice.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
11.2 Si la aplicación de pago facilita el envío de PAN (número de cuenta principal) mediante tecnologías de mensajería del usuario final (por ejemplo, correo electrónico, mensajería instantánea, chat), la aplicación de pago debe proporcionar una solución que convierta el PAN (número de cuenta principal) en ilegible o implemente una criptografía sólida, o especificar el uso de criptografía sólida para cifrar los PAN (número de cuenta principal). ***Concuerda con el Requisito 4.2 de las PCI DSS***	**11.2.a** Si la aplicación de pago permite o facilita el envío de PAN (número de cuenta principal) por medio de tecnologías de mensajería de usuario final, compruebe que se provea una solución que convierta el PAN en ilegible o que implemente una criptografía sólida, o bien, que se especifique cómo utilizarla.	El correo electrónico, la mensajería instantánea y el chat se pueden interceptar fácilmente mediante detectores de paquetes durante la exposición completa de la entrega en redes internas y públicas. No utilice estas herramientas de mensajería para enviar el PAN (número de cuenta principal), a menos que la aplicación de pago implemente una criptografía sólida con estas tecnologías o que convierta el PAN (número de cuenta principal) en ilegible.
	11.2.b Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que se incluyan instrucciones para los clientes y los integradores/revendedores sobre cómo utilizar una solución proporcionada con la aplicación o especificada para utilizar con esta, que incluya los siguientes aspectos: • Procedimientos para utilizar una solución definida para convertir al PAN (número de cuenta principal) en ilegible o para protegerlo con una criptografía sólida. • Instrucciones para que el PAN (número de cuenta principal) quede ilegible o protegido con una criptografía sólida cada vez que se envíe mediante tecnologías de mensajería de usuario final.	
	11.2.c Si se proporciona una solución con la aplicación de pago, instale y evalúe la aplicación para comprobar que la solución convierta el PAN (número de cuenta principal) en ilegible o que implemente una criptografía sólida.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 12: Cifre el acceso administrativo que no sea de consola

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
12.1 Si la aplicación de pago facilita el acceso administrativo sin consola, cifrar todo ese acceso con una criptografía sólida. ***Notas:*** • *Los protocolos de texto claro, como Telnet o rlogin, nunca se deben utilizar para un acceso administrativo.* • *SSL y TLS temprana no se consideran criptografía sólida. Las aplicaciones de pago no deben usar, o apoyar el uso de SSL y TLS temprana. Las aplicaciones que utilizan o soportan TLS no deben permitirse recurrir a SSL.* ***Concuerda con el Requisito 2.3 de las PCI DSS***	**12.1.a** Instale la aplicación de pago en un laboratorio y evalúe las conexiones administrativas que no sean de consola para comprobar que se invoca un método de cifrado sólido antes de solicitar la contraseña del administrador. **12.1.b** Revise los parámetros de configuración de la aplicación de pago para comprobar que no se utilicen protocolos de texto claro, como Telnet y rlogin, para un acceso administrativo que no sea de consola. **12.1.c** Revise la *Guía de implementación de la PA-DSS* preparada por el proveedor y compruebe que incluya instrucciones para los clientes y los integradores/revendedores sobre cómo configurar la aplicación para utilizar criptografía sólida por medio de tecnologías para el cifrado de todo acceso administrativo que no sea de consola.	Si la administración remota no se realiza con una autenticación segura y comunicaciones cifradas, la información confidencial a nivel administrativo u operativo (como las contraseñas del administrador) se puede revelar a un espía. Una persona malintencionada puede utilizar esta información para acceder a la aplicación o a la red, modificar permisos y hurtar datos.
12.1.1 Instruya a los clientes para que cifren todo el acceso administrativo que no sea de consola con tecnologías de criptografía sólida, para la administración basada en la Web u otro acceso administrativo que no sea de consola. ***Nota:*** *Los protocolos de texto claro, como Telnet o rlogin, nunca se deben utilizar para un acceso administrativo.* ***Concuerda con el Requisito 2.3 de las PCI DSS***	**12.1.1** Revise la *Guía de implementación de las PA-DSS* preparada por el proveedor y compruebe que incluya instrucciones para los clientes y los integradores/revendedores para implementar criptografía sólida por medio de tecnologías, para el cifrado de todo acceso administrativo que no sea de consola.	Los proveedores de la aplicación de pago deberán proporcionar instrucciones para que los clientes y los integradores/revendedores utilicen criptografía sólida cuando configuren la aplicación para el cifrado de todo acceso administrativo que no sea de consola. De esta manera, garantizan que se implementen los controles de seguridad de manera adecuada y que se cumplan las directrices de las PA-DSS y de las PCI DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
12,2 Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo. ***Nota:*** *La autenticación de múltiples factores exige utilizar dos de los tres métodos de autenticación (consulte el Requisito 3.1.4 de la PA-DSS para obtener una descripción de los métodos de autenticación).* ***Concuerda con el Requisito 8.3 de las PCI DSS***	**12.2.a** Verifique que se proporciona la autenticación de múltiples factores con la aplicación, o que se especifica el uso del mismo.	El acceso administrativo requiere un mayor nivel de certeza de que la persona que intenta acceder es quien dice ser. Ya que la autenticación de múltiples factores puede ser implementada a nivel de la aplicación, sistema o red, no es necesario que todas las aplicaciones incluyan una solución de autenticación de múltiples factores. Los proveedores de aplicaciones pueden proporcionar la autenticación de múltiples factores con su aplicación, o incluir instrucciones para los usuarios e integradores/revendedores para instalar la autenticación de múltiples factores para el acceso administrativo a la aplicación.
	12.2.b Revise la *Guía de implementación de la PA-DSS* preparada por el proveedor y verifique que incluya instrucciones para los clientes y los integradores/revendedores para que utilicen la autenticación de múltiples factores, incluido: • La indicación que la autenticación de múltiples factores debe ser utilizada por todo el personal con acceso administrativo que no sea de consola al CDE. • Los procedimientos para utilizar la autenticación de múltiples factores proporcionada con la aplicación (si la hubiere).	
	12.2.c Si se proporciona la autenticación de múltiples factores con la aplicación de pago, instale y pruebe la aplicación para verificar que se aplica la autenticación de múltiples factores antes de conceder el acceso.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 13: Mantenga una Guía de implementación de las PA-DSS para los clientes, revendedores e integradores

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
13.1 Desarrolle, mantenga y difunda una *Guía de implementación de las PA-DSS* para clientes, revendedores e integradores que cumpla con lo siguiente:	**13.1** Revise la *Guía de implementación de las PA-DSS* y los procesos del proveedor relacionados y entreviste al personal para comprobar lo siguiente: • La *Guía de implementación de las PA-DSS* se debe distribuir con la aplicación entre todos los clientes, revendedores e integradores. • El proveedor debe disponer de un mecanismo implementado para proporcionar la *Guía de implementación de las PA-DSS* a todos los clientes, revendedores e integradores cuando lo soliciten.	Si la *Guía de implementación de las PA-DSS* está bien diseñada y contiene información detallada, ayudará a los clientes y a los integradores/revendedores a implementar las configuraciones y las medidas de seguridad adecuadas en la aplicación de pago y sus componentes subyacentes para cumplir con las directrices relevantes de las PCI DSS y de las PA-DSS a fin de proteger los datos del titular de la tarjeta.
13.1.1 Proporcionar información específica relevante para que utilicen los clientes, revendedores e integradores de la aplicación.	**13.1.1** Revise la *Guía de implementación de las PA-DSS* y compruebe lo siguiente: • Debe identificar claramente el nombre y la versión de la aplicación de pago a la que se aplica. • Debe proporcionar información detallada de todas las dependencias de la aplicación necesarias para que esta se pueda configurar de manera que cumpla con los requisitos de las PCI DSS.	
13.1.2 Se deben abordan todos los requisitos del presente documento siempre que se haga referencia a la *Guía de implementación de las PA-DSS*.	**13.1.2** Revise la *Guía de implementación de las PA-DSS* y, tomando el Anexo A como referencia, compruebe que la *Guía* considere todos los requisitos relacionados con el presente documento.	
13.1.3 Se debe incluir una revisión, al menos, anual y cada vez que se implementen cambios en la aplicación o en los requisitos de las PA-DSS, y se debe actualizar, según corresponda, para mantener la documentación al día con respecto a los cambios que afectan la aplicación y los requisitos del presente	**13.1.3.a** Revise la *Guía de implementación de las PA-DSS* y entreviste al personal para comprobar que la *Guía* se revise con la siguiente frecuencia: • Por lo menos, anualmente • Cuando se implementen cambios en la aplicación • Cuando se implementen cambios en estos requisitos de la PA-DSS	Cada vez que se implementa una actualización de la aplicación, se introduce o se modifica la funcionalidad del sistema y, en algunos casos, los mecanismos de seguridad críticos de la aplicación. Si la *Guía de implementación de las PA-DSS* no se mantiene actualizada según las últimas versiones

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
documento.	**13.1.3.b** Compruebe que la *Guía de implementación de las PA-DSS* se actualice según corresponda para que se mantenga actualizada con los siguientes cambios: • Cambios en los requisitos de las PA-DSS. • Cambios en la aplicación o en sus dependencias.	de la aplicación de pago, los clientes y los integradores/revendedores pueden omitir controles de seguridad críticos de la aplicación o configurarlos mal, lo que podría permitir a un atacante evadir dichos mecanismos de seguridad y poner en riesgo datos confidenciales.
	13.1.3.c Revise la *Guía de implementación de las PA-DSS* y los procesos relacionados del proveedor y entreviste al personal para comprobar que el proveedor disponga de mecanismos implementados para comunicar las actualizaciones a los clientes, revendedores e integradores y para proporcionar versiones actualizadas cuando sea necesario.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito 14: Asigne responsabilidades según las PA-DSS al personal y establezca programas de capacitación para el personal, los clientes, los revendedores y los integradores

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
14.1 Se debe proporcionar capacitación sobre la seguridad de la información y las PA-DSS , al menos, una vez al año al personal del proveedor con responsabilidad por las PA-DSS.	**14.1** Revise los materiales de capacitación y entreviste al personal responsable para comprobar que todo el personal del proveedor con responsabilidad por las PA-DSS reciba capacitación sobre las PA-DSS y la seguridad de la información, al menos, anualmente.	Para que la aplicación de pago sea diseñada para que cumpla con las directrices de las PA-DSS de manera efectiva, el personal del proveedor de la aplicación de pago debe ser experto en las PA-DSS y en sus responsabilidades respecto de las evaluaciones continuas de las PA-DSS. Es responsabilidad del proveedor de la aplicación de pago garantizar que el personal esté correctamente capacitado en estas áreas.
14.2 Se deben asignar funciones y responsabilidades al personal del proveedor, que incluyan las siguientes tareas: • Responsabilidad general para cumplir con todos los requisitos de las PA-DSS. • Mantenerse actualizado con respecto a los cambios que se implementen en la Guía del programa PA-DSS del PCI SSC. • Asegurar que se sigan prácticas de codificación seguras. • Asegurar que los integradores/revendedores reciban los materiales de capacitación y respaldo. • Asegurar que todo el personal del proveedor	**14.2.a** Revise las responsabilidades documentadas para comprobar que se asigne formalmente la responsabilidad para desempeñar las siguientes funciones: • Responsabilidad general para cumplir con todos los requisitos de las PA-DSS. • Mantenerse actualizado con respecto a los cambios que se implementen en la Guía del programa PA-DSS del PCI SSC. • Asegurar que se sigan prácticas de codificación seguras. • Asegurar que los integradores/revendedores reciban los materiales de capacitación y respaldo. • Asegurar que todo el personal del proveedor que asuma responsabilidades por las PA-DSS, incluidos los desarrolladores, reciban capacitación.	Dentro de cada organización del proveedor de la aplicación de pago, se debe asignar una responsabilidad formal ante las PA-DSS a una parte responsable (ya sea una persona o un equipo) para garantizar que se cumplan todos los requisitos de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
que asuma responsabilidades de las PA-DSS, incluidos los desarrolladores, reciban capacitación.	**14.2.b** Entreviste al personal responsable de las siguientes funciones para confirmar que conocen y comprenden cuáles son dichas funciones y responsabilidades: • Responsabilidad general para cumplir con todos los requisitos de las PA-DSS. • Mantenerse actualizado con respecto a los cambios que se implementen en la Guía del programa PA-DSS del PCI SSC. • Asegurar que se sigan prácticas de codificación seguras. • Asegurar que los integradores/revendedores reciban los materiales de capacitación y respaldo. • Asegurar que todo el personal del proveedor que asuma responsabilidades por las PA-DSS, incluidos los desarrolladores, reciban capacitación.	
14.3 Se deben desarrollar e implementar programas de comunicación y capacitación para los integradores y revendedores de la aplicación de pago. La capacitación debe abarcar, al menos, los siguientes aspectos: • Cómo implementar la aplicación de pago y las redes y sistemas relacionados de manera que cumplan con los requisitos de las PCI DSS. • Cobertura de todos los puntos analizados en la *Guía de implementación de las PA-DSS* en todo este documento (y en el Anexo A).	**14.3.a** Revise los materiales de capacitación para integradores y revendedores, y confirme que incluyan la siguiente información: • Capacitación sobre cómo implementar la aplicación de pago y las redes y sistemas relacionados de manera que cumplan con los requisitos de las PCI DSS. • Cobertura de todos los puntos analizados en la *Guía de implementación de las PA-DSS* en todo este documento (y en el Anexo A).	Si la configuración, el mantenimiento o la asistencia de una aplicación no se realizan correctamente, se podrían generar vulnerabilidades de seguridad en el entorno de datos del titular de la tarjeta del cliente, que luego podrían utilizar los atacantes de manera indebida. Los proveedores de la aplicación deben proporcionar capacitación a los integradores/revendedores sobre la instalación y la configuración seguras de la aplicación para asegurar que, una vez instalada en el entorno del cliente, facilite el cumplimiento con la PCI DSS. Es responsabilidad del proveedor de la aplicación de pago proporcionar capacitación a los integradores y revendedores sobre estas áreas.
	14.3.b Revise los programas de comunicación del proveedor y los procesos relacionados, y entreviste al personal del proveedor para comprobar lo siguiente: • Los integradores y revendedores deben disponer de los materiales de capacitación. • Los proveedores deben contar con un mecanismo implementado para proporcionar materiales actualizados a los integradores y revendedores cuando lo soliciten.	
	14.3.c Entreviste a un grupo de revendedores e integradores para comprobar que hayan recibido la capacitación, con los materiales correspondientes, del proveedor de la aplicación.	
	14.3.d Revise la evidencia de que los integradores y revendedores hayan recibido los materiales de capacitación del proveedor de software.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Procedimientos de prueba	Guía
14.3.1 Revise los materiales de capacitación, al menos, una vez al año y cada vez que se implementen cambios en la aplicación o en los requisitos de las PA-DSS. Actualice los materiales de capacitación según sea necesario para mantener la documentación al día con las nuevas versiones de la aplicación de pago y los cambios implementados en los requisitos de las PA-DSS.	**14.3.1.a** Revise los materiales de capacitación para integradores y revendedores, y compruebe que cumplan con los siguientes requisitos: • Se debe revisar, al menos, una vez al año y cada vez que se implementen cambios en la aplicación o en los requisitos de las PA-DSS. • Se debe actualizar según sea necesario para mantener la documentación al día con las nuevas versiones de la aplicación de pago y los cambios implementados en los requisitos de las PA-DSS.	Los materiales de capacitación para el personal del proveedor de la aplicación de pago, los integradores y los revendedores se deben actualizar, al menos, una vez al año para garantizar que se mantenga al día con las últimas versiones de las aplicaciones y con los requisitos de las PA-DSS. Si se utilizan materiales de capacitación desactualizados, los programas de capacitación podrían ser ineficientes, lo que ocasionaría que los integradores y revendedores diseñen funciones de seguridad deficientes dentro de la aplicación o configuraciones de aplicaciones inapropiadas.
	14.3.1.b Revise el proceso de distribución para las nuevas versiones de la aplicación de pago y compruebe que la documentación actualizada se distribuya a los integradores y a los revendedores junto con la aplicación de pago actualizada.	
	14.3.1.c Entreviste a un grupo de revendedores e integradores para comprobar que hayan recibido los materiales de capacitación actualizados del proveedor de la aplicación.	

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

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* proporcionada a los clientes y a los integradores/revendedores (consulte la página 11 de la "Guía de implementación de las PA-DSS") y describir las responsabilidades de implementar los controles relacionados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio 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.	Se deben proporcionar las siguientes instrucciones a los clientes y a los integradores/revendedores: ▪ Se deben eliminar los datos históricos (contenido de la pista, códigos de verificación de tarjeta, PIN o bloqueos de PIN almacenados en 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.	**Proveedor de software**: Proporcione la herramienta o el procedimiento para que los clientes puedan eliminar de manera segura los datos de autenticación confidenciales almacenados en versiones anteriores, de acuerdo con el Requisito 1.1.4 de las PA-DSS. **Clientes e integradores/revendedores**: Borre todos los datos históricos de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 1.1.4 de las PA-DSS.
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.	Se deben proporcionar las siguientes instrucciones a los clientes y a los integradores/revendedores: ▪ Los datos de autenticación confidenciales (autorización previa) solamente se deben reunir cuando sea necesario resolver un problema específico. ▪ Dichos datos solo se deben almacenar en ubicaciones específicas, conocidas y con acceso limitado. ▪ Reúna solo una cantidad limitada de datos necesarios para resolver un problema específico. ▪ Los datos de autenticación confidenciales se deben cifrar al momento de almacenarlos. ▪ Dichos datos se deben borrar de manera segura e inmediatamente después de utilizarlos.	**Proveedor de software**: No almacene datos de autenticación confidenciales; resuelva cualquier problema de los clientes de acuerdo con el Requisito 1.1.5.a de las PA-DSS. **Clientes e integradores/revendedores:** No almacene datos de autenticación confidenciales; resuelva cualquier problema de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 1.1.5.a de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
2.1	Elimine los datos del titular de la tarjeta de manera segura después del período de retención definido por el cliente.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Instrucciones para eliminar 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 los datos del titular de la tarjeta, para que el cliente sepa las ubicaciones de los datos que se deben eliminar. ▪ Instrucciones que los clientes necesitan para eliminar los datos del titular de la tarjeta de modo seguro cuando ya no sean necesarios para fines legales, reglamentarios o comerciales. ▪ Cómo eliminar de modo seguro los datos del titular de la tarjeta almacenados por la aplicación de pago, incluidos los datos almacenados en el software o en los sistemas subyacentes (como OS, bases de datos, etc.). ▪ Cómo configurar el software o los sistemas subyacentes (como OS, bases de datos, etc.) para impedir la captura o la retención involuntaria de datos del titular de la tarjeta.	**Proveedor de software**: Infórmeles a los clientes que los datos del titular de la tarjeta que excedan los períodos de retención definidos por el cliente se deben eliminar de modo seguro de las ubicaciones de la aplicación de pago donde se almacenen y de los sistemas o software subyacentes, y cómo eliminar de modo seguro los datos del titular de la tarjeta almacenados por la aplicación de pago. **Clientes e integradores/revendedores**: Elimine de manera segura los datos del titular de la tarjeta que excedan el período de retención definido por el cliente, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 2.1 de las PA-DSS.
2.2	Se debe ocultar el PAN cuando aparezca para que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis y los últimos cuatro dígitos del PAN.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Detalles de todas las instancias en las que se muestra el PAN, que incluyen, entre otras, los dispositivos de POS, las pantallas, los registros y los recibos. ▪ Confirmación de que la aplicación de pago oculta el PAN de manera predeterminada en todas las vistas. ▪ Instrucciones sobre cómo configurar la aplicación de pago de modo que solo el personal con una necesidad comercial legítima pueda ver el PAN (número de cuenta principal) completo.	**Proveedor de software**: Proporcione instrucciones a los clientes para que oculten el PAN (número de cuenta principal), de modo que solo el personal con una necesidad comercial legítima pueda verlo completo. **Clientes e integradores/revendedores**: Oculte las vistas del PAN (número de cuenta principal), de modo que solo el personal con una necesidad comercial legítima pueda verlo completo, de acuerdo con la *Guía de implementación de la PA-DSS* y el Requisito 2.2 de la PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
2.3	Convierta el PAN (número de cuenta principal) en 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).	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Detalles de cualquier opción que pueda ser configurada para cada método que utiliza la aplicación para hacer que los datos del titular de la tarjeta sean ilegibles, e instrucciones sobre cómo configurar cada método para todas las ubicaciones donde la aplicación de pago almacene datos de los titulares de la tarjeta (de acuerdo con el Requisito 2.1 de las PA-DSS). ▪ Una lista de todas las instancias en que los datos del titular de la tarjeta puedan extraerse de la aplicación de pago para que el cliente los almacene fuera de esta, e instrucciones que el cliente debe seguir para hacer que los PAN sean ilegibles en tales instancias. ▪ La indicación de que si los registros de depuración se activan (por ejemplo, para solucionar problemas), y los registros incluyen el PAN, se deben proteger de conformidad con la PCI DSS, desactivarlos tan pronto como se haya completado la resolución de problemas, y eliminarlos de manera segura cuando ya no sean necesarios.	**Proveedor de software**: Proporcione instrucciones a los clientes para que conviertan el PAN (número de cuenta principal) en ilegible en todo lugar donde se almacene o cuando se extraiga de la aplicación de pago. **Clientes e integradores/revendedores**: Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 2.3 de las PA-DSS.
2.4	Proteja las claves utilizadas para asegurar los datos de los titulares de tarjeta contra divulgación o uso indebido.	Se deben proporcionar las siguientes instrucciones a los clientes y a los integradores/revendedores: ▪ 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.	**Proveedor de software**: Infórmeles a los clientes que las claves utilizadas para proteger los datos del titular de la tarjeta se deben almacenar, de modo seguro, en la menor cantidad de ubicaciones posibles, y el acceso a dichas claves debe estar restringido a la menor cantidad de custodios posibles. **Clientes e integradores/revendedores**: Almacene las claves de modo seguro en la menor cantidad de ubicaciones posibles, con acceso restringido a la menor cantidad de custodios posibles, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 2.4 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
2.5	Implemente los procesos y los procedimientos de administración de claves criptográficas que se utilizan para el cifrado de los datos del titular de la tarjeta.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Instrucciones sobre cómo generar, distribuir, proteger, cambiar, almacenar y retirar o reemplazar claves de cifrado cuando los clientes o integradores/revendedores participan en estas actividades de administración de claves. ▪ Un formulario de Custodio de claves para que los custodios de las claves reconozcan que entienden y aceptan sus responsabilidades.	**Proveedor de software**: Infórmeles a los clientes que acceden a claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta que implementen procesos y procedimientos de administración de claves. **Clientes e integradores/revendedores**: Implemente los procesos y los procedimientos de administración de claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 2.5 de las PA-DSS.
2.5.1 a 2.5.7	Implemente funciones para la administración segura de claves.	Infórmeles a los clientes y a los integradores/revendedores cómo desarrollar funciones de administración de claves, e incluya la siguiente información: ▪ Generación de claves criptográficas sólidas. ▪ Distribución segura de claves criptográficas. ▪ Almacenamiento seguro de claves criptográficas. ▪ Cambios de claves criptográficas que han llegado al final de su período de cifrado. ▪ Retiro o reemplazo de claves, según se considere necesario, cuando se haya debilitado la integridad de la clave o se sospeche que las claves pueden estar en riesgo. ▪ Conocimiento dividido y control doble de las operaciones manuales de administración de claves criptográficas en texto claro admitidas por la aplicación. ▪ Prevención de la sustitución no autorizada de claves criptográficas.	**Proveedor de software**: Infórmeles a los clientes que deben implementar funciones para la administración segura de claves. **Clientes e integradores/revendedores**: Implemente funciones para la administración segura de claves para las claves criptográficas de acuerdo con la *Guía de implementación de las PA-DSS* y los Requisitos 2.5.1 a 2.5.7 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
2.6	Proporcione un mecanismo para que no se pueda recuperar ningún material de clave criptográfica o criptograma almacenado por la aplicación de pago.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Procedimientos que detallen cómo usar las herramientas o los procedimientos suministrados con la aplicación para hacer que el material criptográfico sea irrecuperable. ▪ Instrucciones para que, cuando las claves ya no se utilicen, los materiales de claves criptográficas no se puedan recuperar, de acuerdo con los requisitos de administración de claves de las PCI DSS. ▪ Instrucciones sobre cómo volver a cifrar datos históricos con claves nuevas, incluidos los procedimientos para mantener la seguridad de los datos en texto claro durante los procesos de descifrado/recifrado.	**Proveedor de software**: Proporcione la herramienta o el procedimiento para eliminar de modo seguro el material de claves criptográficas o los criptogramas almacenados por la aplicación, y facilite la herramienta o el procedimiento para volver a cifrar los datos históricos con claves nuevas. **Clientes e integradores/revendedores**: Elimine todo el material criptográfico histórico de acuerdo con los requisitos de administración de claves de la *Guía de implementación de las PA-DSS* y el Requisito 2.6 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio 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.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Instrucciones sobre cómo la aplicación de pago implementa una autenticación sólida para todas las credenciales de autenticación (por ejemplo, usuarios, contraseñas) que la aplicación genera o administra por uno de los siguientes medios: - Aplicar cambios seguros a las credenciales de autenticación una vez que finaliza la instalación de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS. - Aplicar cambios seguros a las credenciales de autenticación para cualquier cambio posterior (después de la instalación) de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS. ▪ Recomendación en la que se sugiera que, para mantener el cumplimiento de las PCI DSS, se debe verificar que los cambios implementados en las configuraciones de autenticación proporcionen métodos de autenticación que sean tan estrictos como los requisitos de las PCI DSS. ▪ Asignar una autenticación segura a todas las cuentas predeterminadas en el entorno ▪ Recomendación de asignar autenticación segura a cualquier cuenta predeterminada (aún cuando no se utilice) y, luego, desactivar las cuentas o no utilizarlas. ▪ Cómo cambiar y crear credenciales de autenticación cuando esas credenciales no son generadas ni administradas por la aplicación de pago, de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS, al concluir la instalación y para cambios posteriores después de la instalación, para todas las cuentas a nivel de aplicación con acceso administrativo o con acceso a datos del titular de la tarjeta. ▪ La identificación de todas las funciones y las cuentas predeterminadas dentro de la aplicación con acceso administrativo.	**Proveedor de software**: En el caso de todas las credenciales de autenticación generadas o administradas por la aplicación, asegúrese de que la aplicación de pago exija a los clientes el uso de ID de usuario exclusivas y autenticación segura para cuentas/contraseñas, de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS. En el caso de las credenciales de autenticación no generadas ni administradas por la aplicación de pago, asegúrese de que la *Guía de implementación de las PA-DSS* proporcione a los clientes y a los integradores/revendedores orientación clara y precisa sobre cómo cambiar y crear credenciales de autenticación seguras de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS. **Clientes e integradores/revendedores**: Establezca y mantenga ID de usuario exclusivas y una autenticación segura de acuerdo con la *Guía de implementación de las PA-DSS* y los Requisitos 3.1.1 a 3.1.11 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
3.2	Utilice ID de usuario únicos y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago.	Instruya a los clientes y a los integradores/revendedores para que utilicen nombres de usuario exclusivos y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago o datos del titular de la tarjeta, de acuerdo con los Requisitos 3.1.1 a 3.1.11 de las PA-DSS.	**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. **Clientes e integradores/revendedores**: Establezca y mantenga ID de usuario exclusivas y una autenticación segura de acuerdo con la *Guía de implementación de las PA-DSS* y los Requisitos 3.1.1 a 3.1.11 de las PA-DSS.
4.1	Implemente pistas de auditoría automatizadas.	Proporcione instrucciones para implementar pistas de auditoría automatizadas que incluyan los siguientes aspectos: ▪ Cómo instalar la aplicación para que los registros estén configurados y activados de manera predeterminada al completar el proceso de instalación. ▪ Cómo establecer valores de configuración del registro que cumplan con las PCI DSS, según los Requisitos 4.2, 4.3 y 4.4 de las PA-DSS, para todas las opciones de registro que el cliente pueda configurar después de la instalación. ▪ Se deben activar los registros, ya que desactivarlos provocará un incumplimiento de las PCI DSS. ▪ Cómo establecer los valores de configuración del registro para que cumplan con las PCI para cualquier componente de software de terceros empaquetado o requerido por la aplicación de pago, para todas las opciones de registro que el cliente pueda configurar después de la instalación.	**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. **Clientes e integradores/revendedores:** Establezca y mantenga registros que cumplan con las PCI DSS de acuerdo con la *Guía de implementación de las PA-DSS* y los Requisitos 4.2, 4.3 y 4.4 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
4.4	Facilite el registro centralizado.	Proporcione una descripción sobre cuáles son los mecanismos de registro centralizados admitidos, e instrucciones y procedimientos para incorporar los registros de la aplicación de pago a un servidor de registro centralizado.	**Proveedor de software**: Asegúrese de que la aplicación de pago admita el registro centralizado en entornos de clientes, de acuerdo con el Requisito 4.4 de las PA-DSS. **Clientes e integradores/revendedores:** Establezca y mantenga un registro centralizado de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 4.4 de las PA-DSS.
5.4.4	Implemente una metodología de control de versiones de la aplicación y comuníquela.	Proporcione una descripción de la metodología de control de versiones publicada del proveedor e incluya orientación sobre los siguientes aspectos: ▪ Información detallada sobre el esquema de control de versiones, que incluya el formato del esquema de la versión (cantidad de elementos, separadores, conjunto de caracteres, etc.). ▪ Información detallada sobre cómo se indicarán los cambios que afectan la seguridad en el esquema de control de versiones. ▪ Información detallada sobre cómo afectarán la versión otros tipos de cambios. ▪ Información detallada sobre los elementos comodines que se utilizan, que indique que estos nunca se utilizarán para representar un cambio que afecte la seguridad.	**Proveedor de software**: Documente e implemente una metodología de control de versiones del software como parte del ciclo de vida de desarrollo del sistema. La metodología debe seguir los procedimientos que se detallan en la *Guía del programa PA-DSS* para los cambios que se implementen en las aplicaciones, de acuerdo con el Requisito 5.5 de las PA-DSS. **Clientes e integradores/revendedores:** Deben entender qué versión de la aplicación de pago están utilizando y asegurarse de utilizar las versiones validadas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
6.1	Implemente tecnología inalámbrica de manera segura.	En cuanto a las aplicaciones de pago desarrolladas para utilizar con tecnología inalámbrica, los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Instrucciones sobre cómo la aplicación de pago exige cambios en las claves de cifrado, en las contraseñas y en las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas durante la instalación para todos los componentes inalámbricos controlados por la aplicación. ▪ Procedimientos para cambiar las contraseñas y las claves de cifrado inalámbricas, incluidas las cadenas SNMP, cada vez que una persona que conozca las claves/contraseñas cesa en sus funciones o se traslada a otro cargo en la empresa. ▪ Instrucciones para cambiar las claves de cifrado, las contraseñas y las cadenas comunitarias SNMP predeterminadas de cualquier componente inalámbrico proporcionado por la aplicación pero que esta no controle. ▪ Instrucciones para instalar un firewall entre las redes inalámbricas y los sistemas que almacenen datos del titular de la tarjeta. ▪ Información detallada de todo el tráfico inalámbrico (que incluya información específica de la información de puerto) que utilizaría la función inalámbrica de la aplicación de pago. ▪ Instrucciones para configurar los firewalls para que nieguen o (si el tráfico es necesario para fines comerciales) permitan solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	**Proveedor de software**: Asesore a los clientes y a los revendedores/integradores para que, de acuerdo 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 inalámbrica con la aplicación de pago. **Clientes e integradores/revendedores**: En el caso de la tecnología inalámbrica implementada por los clientes o los integradores/revendedores dentro del entorno de pagos, cambie los valores predeterminados del proveedor de acuerdo con el Requisito 6.1 de las PA-DSS e instale un firewall de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 2.1.1 de las PCI DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
6.2	Asegure las transmisiones de datos de titulares de tarjetas que se realizan mediante redes inalámbricas.	En el caso de las aplicaciones de pago desarrolladas para utilizar con tecnologías inalámbricas, incluya instrucciones a fin de utilizar las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) para implementar un cifrado sólido para la autenticación y la transmisión de datos del titular de la tarjeta. Esto incluye los siguientes aspectos: ▪ Cómo configurar la aplicación para que utilice las mejores prácticas de la industria (por ejemplo, IEEE 802.11.i) a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión. ▪ Cómo configurar todas las aplicaciones inalámbricas combinadas con la aplicación de pago para que utilice las mejores prácticas de la industria, a los efectos de proporcionar cifrados sólidos para la autenticación y transmisión.	**Proveedor de software**: Asesore a los clientes y a los revendedores/integradores para que, si utilizan tecnología inalámbrica con la aplicación de pago, implementen transmisiones cifradas seguras, de acuerdo con el Requisito 6.2 de las PA-DSS. **Clientes e integradores/revendedores**: Para la tecnología inalámbrica implementada en el entorno de pagos por clientes o integradores/revendedores, utilice transmisiones cifradas seguras de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 6.2 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
6.3	Proporcione instrucciones para el uso seguro de la tecnología inalámbrica.	Proporcione instrucciones para que los valores de configuración inalámbricos cumplan con las PCI DSS, e incluya la siguiente información: ▪ Instrucciones para cambiar todas las claves de cifrado, las contraseñas y las cadenas comunitarias SNMP predeterminadas al momento de la instalación. ▪ Instrucciones para cambiar las contraseñas, las claves de cifrado y las cadenas SNMP inalámbricas, cada vez que una persona que conozca las claves/contraseñas cesa en sus funciones o se traslada a otro cargo en la empresa. ▪ Instrucciones para instalar un firewall entre las redes inalámbricas y los sistemas que almacenan datos del titular de la tarjeta, y para configurar los firewalls para negar el tráfico o controlarlo (si es necesario para fines comerciales) desde el entorno inalámbrico hacia el entorno de datos del titular de la tarjeta. ▪ Instrucciones para utilizar las mejores prácticas de la industria (por ej., IEEE 802.11i) para proporcionar cifrado sólido para la autenticación y la transmisión.	**Proveedor de software**: Asesore a los clientes y a los integradores/revendedores para que protejan las tecnologías inalámbricas de acuerdo con el Requisito 6.3 de las PA-DSS. **Clientes e integradores/revendedores**: Proteja las tecnologías inalámbricas de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 6.2 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
7.2.3	Proporcionar instrucciones para los clientes acerca de la instalación segura de parches y actualizaciones.	Los clientes y los integradores/revendedores deben contar con la siguiente información: • Cómo el proveedor comunicará las notificaciones de los nuevos parches y actualizaciones. • Cómo se entregarán los parches y actualizaciones de una manera segura con una cadena de confianza conocida. • Cómo acceder e instalar parches y actualizaciones de una manera que mantenga la integridad del código de parche y de actualización.	**Proveedor de software:** Documentar e implementar los procesos de comunicación, entrega e instalación segura de parches y actualizaciones. **Clientes e integradores/revendedores:** Acceder e instalar parches y actualizaciones de manera segura, de acuerdo con la *Guía de implementación de la PA-DSS*.
8.2	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.	**Proveedor de software:** Asegúrese de que la aplicación de pago admita que el cliente utilice solo los protocolos, servicios, etc., seguros y necesarios al 1) tener solo protocolos, servicios, etc., necesarios, activados por opción predeterminada, 2) tener dichos protocolos, servicios, etc., necesarios, configurados de forma segura por opción predeterminada y 3) al documentar los protocolos, servicios, etc., necesarios, como referencia para clientes y para integradores/revendedores. **Clientes e integradores/revendedores:** Utilice la lista documentada de la *Guía de implementación de las PA-DSS* para asegurarse de que solo se utilicen en el sistema protocolos, servicios, etc., necesarios y seguros, de acuerdo con el Requisito 5.4 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
9.1	Almacene datos de titulares de tarjetas únicamente en los servidores que no estén conectados a Internet.	Los clientes y los integradores/revendedores deben contar con la siguiente información: ▪ Instrucciones de no almacenar datos del titular de la tarjeta en sistemas públicos (por ejemplo, el servidor web y el servidor de base de datos no deben estar en el mismo servidor). ▪ Instrucciones sobre cómo configurar la aplicación de pago para utilizar una DMZ (zona desmilitarizada) para separar Internet de los sistemas que almacenan datos del titular de la tarjeta. ▪ Una lista de los servicios/puertos que necesita utilizar la aplicación para comunicar entre dos zonas de red (para que el cliente pueda configurar sus firewalls para que abran solo los puertos requeridos).	**Proveedor de software**: Asegúrese de que la aplicación de pago no requiera el almacenamiento de datos del titular de la tarjeta en la DMZ (zona desmilitarizada) ni en sistemas accesibles desde Internet ni permita el uso de una DMZ (zona desmilitarizada) de acuerdo con el Requisito 9 de las PA-DSS. **Clientes e integradores/revendedores**: 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 *Guía de implementación de las PA-DSS* y el requisito 9 de las PA-DSS.
10.1	Implemente la autenticación de múltiples factores para todos los accesos remotos a la aplicación de pago que se origine fuera del entorno de cliente.	Proporcione a los clientes y los integradores/revendedores la siguiente información: ▪ Instrucciones que indiquen que todos los accesos remotos que se originan fuera de la red del cliente hacia la aplicación de pago deben utilizar la autenticación de múltiples factores para cumplir con los requisitos de las PCI DSS. ▪ Una descripción de los mecanismos de la autenticación de múltiples factores admitidos por la aplicación. ▪ Instrucciones para configurar la aplicación para que admita la autenticación de múltiples factores (al menos dos de los tres métodos de autenticación descritos en el Requisito 3.1.4 de la PA DSS).	**Proveedor de software**: Asegúrese de que la aplicación de pago admita que el cliente utilice una autenticación de múltiples factores para todos los accesos remotos a la aplicación de pago que se originen fuera del entorno de cliente, de acuerdo con el Requisito 10.2 de la PA-DSS. **Clientes e integradores/revendedores**: Establezca y mantenga una autenticación de múltiples factores para todos los accesos remotos a la aplicación de pago que se originen fuera del entorno de cliente, de acuerdo con la *Guía de implementación de la PA-DSS* y el Requisito 10.2 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
10.2.1	Entregue de manera segura las actualizaciones de la aplicación de pago.	Si las actualizaciones de la aplicación de pago se envían mediante acceso remoto a los sistemas de los clientes, proporcione la siguiente información: ▪ Instrucciones para activar las tecnologías de acceso remoto para actualizaciones de la aplicación de pago solo cuando sea necesario para descargas, y para desactivarlas de inmediato después de terminar la descarga, de acuerdo con el Requisito 12.3.9 de las PCI DSS. ▪ Instrucciones para que, si la computadora está conectada mediante una VPN (red privada virtual) u otra conexión de alta velocidad, reciba actualizaciones remotas de la aplicación de pago por medio de un firewall personal o de un firewall configurado de manera segura, de acuerdo con el Requisito 1 de las PCI DSS.	**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. **Clientes e integradores/revendedores**: Reciba de manera segura de parte del proveedor las actualizaciones de la aplicación de pago, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 10.3 de las PA-DSS y el Requisito 1 de las PCI DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
10.2.3	Implemente de manera segura un software de acceso remoto.	Incluya instrucciones para que todos los accesos remotos a la aplicación de pago se implementen de modo seguro, por ejemplo: ▪ 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 a 3.1.11 de las PA-DSS). ▪ Activar la transmisión de datos cifrados de acuerdo con el Requisito 12.1 de las PA-DSS. ▪ Activar el bloqueo de cuenta después de una determinada cantidad de intentos fallidos de inicio de sesión (consulte el Requisito 3.1.9 a 3.1.10 de las PA-DSS). ▪ Establecer una conexión VPN (red privada virtual) a través de un firewall antes de permitir el acceso. ▪ Activar la función de inicio de sesión. ▪ Restringir el acceso a entornos de clientes a personal autorizado de los integradores/revendedores.	**Proveedor de software**: (1) Si el proveedor puede acceder remotamente a las aplicaciones de pago de los clientes, implemente el acceso remoto de manera segura según se especifica en el Requisito 10.3.2 de las PA-DSS. (2) Asegúrese de que la aplicación de pago admita que los clientes utilicen funciones de seguridad de acceso remoto. **Clientes e integradores/revendedores**: Utilice funciones de seguridad de acceso remoto para todas las aplicaciones de pago con acceso remoto, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 10.3.2 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio 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.	Si la aplicación de pago envía o facilita el envío de datos del titular de la tarjeta por redes públicas, incluya instrucciones para implementar y utilizar criptografía sólida y protocolos de seguridad para transmisiones seguras de los datos del titular de la tarjeta por estas redes, que incluyan la siguiente información: ▪ Uso obligatorio de criptografía sólida y de protocolos de seguridad, siempre que los datos del titular de la tarjeta se transmitan por redes públicas. ▪ Instrucciones para comprobar que solo se acepten claves o certificados de confianza. ▪ Cómo configurar la aplicación de pago para utilizar solo versiones seguras e implementaciones seguras de los protocolos de seguridad. ▪ Cómo configurar la aplicación de pago para evitar el retroceso a una versión insegura o configuración (por ejemplo, si se utiliza TLS, la aplicación no debe permitirse recurrir a SSL). ▪ Cómo configurar la aplicación de pago para utilizar la solidez de cifrado adecuada según la metodología de cifrado que se utilice.	**Proveedor de software**: Asegúrese de que la aplicación de pago admita que el cliente utilice criptografía sólida y protocolos de seguridad para transmisiones de datos del titular de la tarjeta por redes públicas, de acuerdo con el Requisito 11.1 de las PA-DSS. **Clientes e integradores/revendedores**: Establezca y mantenga una criptografía sólida y protocolos de seguridad para transmisiones de datos del titular de la tarjeta, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 11.1 de las PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
11.2	Cifre los datos de titulares de tarjetas por medio de tecnologías de mensajería de usuario final.	Si la aplicación de pago facilita el envío de PAN (número de cuenta principal) por medio de tecnologías de mensajería de usuario final, incluya instrucciones para implementar y utilizar una solución que convierta el PAN (número de cuenta principal) en ilegible o que implemente una criptografía sólida, e incluya la siguiente información: ▪ Procedimientos para utilizar una solución definida para convertir al PAN (número de cuenta principal) en ilegible o para proteger el PAN (número de cuenta principal) con una criptografía sólida. ▪ Instrucciones para que el PAN (número de cuenta principal) quede ilegible o protegido con una criptografía sólida cada vez que se envíe mediante tecnologías de mensajería de usuario final.	**Proveedor de software**: Proporcione o especifique el uso de una solución que convierta el PAN (número de cuenta principal) en ilegible o implemente una criptografía sólida, y asegúrese de que la aplicación de pago admita que el cliente cifre o convierta en ilegible el PAN (número de cuenta principal) en caso de enviarlo por medio de tecnologías de mensajería de usuario final, de acuerdo con el Requisito 11.2 de las PA-DSS. **Clientes e integradores/revendedores**: Cifre todos los PAN (número de cuenta principal) enviados por medio de tecnologías de mensajería de usuario final con criptografía sólida, o conviértalos en ilegibles, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 11.2 de las PA-DSS.
12.1	Cifre el acceso administrativo que no sea de consola.	Si la aplicación de pago facilita el acceso administrativo que no sea de consola, incluya instrucciones sobre cómo configurar la aplicación para utilizar una criptografía sólida para el cifrado de todo acceso administrativo que no sea de consola a la aplicación de pago o a servidores en el entorno de datos del titular de la tarjeta.	**Proveedor de software**: Si la aplicación de pago facilita el acceso administrativo que no sea de consola, asegúrese de que la aplicación de pago implemente un cifrado sólido para el acceso administrativo que no sea de consola, de acuerdo con el Requisito 12.1 de las PA-DSS. **Clientes e integradores/revendedores**: Cifre todo el acceso administrativo que no sea de consola, de conformidad con la *Guía de implementación de la PA-DSS* y el requisito 12.1 de la PA-DSS.
12.1.1	Cifre el acceso administrativo que no sea de consola.	Incluya instrucciones para los clientes y los integradores/revendedores para que implementen criptografía sólida para el cifrado de todo acceso administrativo que no sea de consola.	**Proveedor de software**: Asegúrese de que la aplicación de pago admita que el cliente cifre todo acceso administrativo que no sea de consola, de acuerdo con el Requisito 12.1.1. de la PA-DSS. **Clientes e integradores/revendedores**: Cifre todo el acceso administrativo que no sea de consola, de acuerdo con la *Guía de implementación de las PA-DSS* y el Requisito 12.1.1. de la PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisitos de las PA-DSS	Tema de las PA-DSS	Contenido obligatorio de la Guía de implementación	Responsable de la implementación de controles
12.2	Incorpore la autenticación de múltiples factores para todo acceso que no sea de consola para el personal con acceso administrativo.	Incluir instrucciones para los clientes y los integradores/revendedores para utilizar la autenticación de múltiples factores, incluido: • La indicación de que la autenticación de múltiples factores debe ser utilizada para todo el personal con acceso administrativo sin consola al CDE. • Los procedimientos para utilizar la autenticación de múltiples factores proporcionada con la aplicación (si la hubiere).	**Proveedor de software**: Garantizar que la aplicación de pago ofrece o especifica el uso de la autenticación de múltiples factores para todo el personal con acceso administrativo sin consola, de acuerdo con el Requisito 12.2. de la PA-DSS. **Clientes e integradores/revendedores**: Utilice la autenticación de múltiples factores para todo el acceso administrativo que no sea de consola, de acuerdo con la *Guía de implementación de la PA-DSS* y el Requisito 12.2 de la PA-DSS.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Anexo B: Configuración del laboratorio de pruebas para la evaluación de las PA-DSS

Para cada evaluación de las PA-DSS que se lleve a cabo, el PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe confirmar el estado y las capacidades del laboratorio utilizado para llevar a cabo las pruebas para la evaluación de las PA-DSS. Esta confirmación se debe enviar junto con el *ROV (informe de validación)* completo.

Para cada procedimiento de validación del laboratorio, el PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe 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 (asesor de seguridad certificado para las aplicaciones de pago) o el laboratorio del proveedor de software. Los PA-QSA (asesores de seguridad certificados para las aplicaciones de pago) deben mantener un laboratorio de pruebas que cumpla con todos los requisitos que se detallan a continuación y deben utilizar su propio laboratorio para llevar a cabo evaluaciones siempre que sea posible. El laboratorio del proveedor de software solo se puede utilizar cuando sea necesario (por ejemplo, el PA-QSA [asesor de seguridad certificado para las aplicaciones de pago] no cuenta con el sistema mainframe, AS400, ni el Tandem en el que se ejecuta la aplicación de pago) y después de comprobar que cumpla con todos los requisitos del laboratorio.

El PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe confirmar todos los puntos de la siguiente tabla y cumplir los siguientes requisitos:

- **Identificación de la ubicación y del propietario del (de los) laboratorio(s) utilizado(s) para realizar la revisión de las PA-DSS.**
- **Descripción de la arquitectura de las pruebas del laboratorio y del entorno implementado para la revisión de las PA-DSS.**
- **Descripción de cómo se simuló el uso real de la aplicación de pago en el laboratorio para esta revisión de las PA-DSS.**

La *Plantilla para crear informes ROV (informe de validación) según las PA-DSS* proporciona detalles de la validación del laboratorio, la cual debe proporcionarse para cada evaluación.

Requisito del laboratorio	Procedimiento de validación del laboratorio
1. Instale la aplicación de pago según las instrucciones de instalación del proveedor o según la capacitación provista al cliente.	**1.** Compruebe que el manual de instalación del proveedor o la capacitación proporcionada a los clientes se haya utilizado para realizar la instalación predeterminada del producto de la aplicación de pago en todas las plataformas enumeradas en el informe de PA-DSS para simular la experiencia real del cliente.
2. Instale y pruebe todas las versiones de la aplicación de pago publicadas en el informe de PA-DSS.	**2.a** Compruebe 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.
	2.b Compruebe que se hayan evaluado todas las plataformas y versiones de la aplicación de pago, incluidos todos los componentes y las dependencias necesarios del sistema.
	2.c Compruebe que se hayan evaluado todas las funcionalidades críticas de la aplicación de pago en cada versión.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito del laboratorio	Procedimiento de validación del laboratorio
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.
4. Instale y/o configure todos los valores de configuración de seguridad requeridos por las PCI DSS.	**4.** Compruebe 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.
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.
	5.b El laboratorio utiliza solo los números de tarjeta de prueba para la simulación/prueba; no se utilizan PAN activos para las pruebas. ***Nota:*** *Las tarjetas de prueba se pueden obtener del proveedor o de un procesador o adquiriente.*
	5.c El laboratorio ejecuta las funciones de autorización o liquidación de la aplicación de pago y se examinan los resultados según el punto 6 que aparece más abajo.
	5.d El laboratorio 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.
	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.
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.[6]

[6] 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.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito del laboratorio	Procedimiento de validación del laboratorio
	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 acuerdo con el Requisito 5.2 de las PA-DSS.
	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 7.2.2 de las PA-DSS.
7. Utilice el laboratorio del proveedor ÚNICAMENTE después de verificar que se cumplan todos los requisitos.	Si se necesita utilizar el laboratorio del proveedor de software (por ejemplo, el PA-QSA [asesor de seguridad certificado para las aplicaciones de pago] no cuenta con el sistema mainframe, AS400, ni el Tandem en el que se ejecuta la aplicación de pago), el PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) 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 (asesor de seguridad certificado para las aplicaciones de pago) debe verificar que el equipo y el laboratorio del proveedor cumplan con los siguientes requisitos:
	7.a El PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe verificar que el laboratorio del proveedor cumpla con todos los requisitos antes mencionados y especificados en este documento, y debe documentar los detalles del informe.
	7.b El PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe validar la instalación adecuada del entorno de laboratorio remoto para asegurarse de que este simule fielmente una situación real y que el proveedor no haya modificado ni alterado el entorno de ninguna manera.
	7.c Todas las pruebas deben ser ejecutadas por el PA-QSA (asesor de seguridad certificado para las aplicaciones de pago); el proveedor no puede ejecutar pruebas respecto de su propia aplicación.
	7.d Todas las pruebas (1) se realizarán in situ en el local del proveedor o (2) se realizarán de manera remota mediante una conexión de red utilizando un vínculo seguro (por ejemplo, una VPN).
	7.e Utilice únicamente números de tarjetas de prueba para simulación/prueba; no utilice PAN (número de cuenta principal) activos para las pruebas. Estas tarjetas de prueba se pueden obtener del proveedor o de un procesador o adquirente.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.

Requisito del laboratorio	Procedimiento de validación del laboratorio
8. Mantenga un proceso de QA (control de calidad) eficiente.	**8.a** El personal de QA (control de calidad) del PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe comprobar que se incluyan todas las plataformas y versiones identificadas en el informe de PA-DSS que aparece en las pruebas.
	8.b El personal de QA (control de calidad) del PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe comprobar que se evalúen todos los requisitos de las PA-DSS.
	8.c El personal de QA (control de calidad) del PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) debe comprobar que las configuraciones y los procesos del laboratorio del PA-QSA (asesor de seguridad certificado para las aplicaciones de pago) cumplan con los requisitos y se documenten con precisión en el informe.
	8.d El personal de QA del PA-QSA debe verificar que el informe muestre con precisión los resultados de las pruebas.

© 2006-2016 Consejo sobre Normas de Seguridad de la PCI, LLC. Todos los derechos reservados.