Industria de Tarjetas de Pago (PCI)
Normas de seguridad de datos

Requisitos y procedimientos de evaluación de seguridad

Versión 1.2.1

Julio de 2009

Modificaciones realizadas al documento

Fecha	Versión	Descripción	Páginas
Octubre de 2008	*1.2*	*Introducir las PCI DSS versión 1.2 como "Requisitos y procedimientos de evaluación de seguridad de las PCI DSS", con lo que se elimina la redundancia entre documentos, y hacer cambios tanto generales como específicos de los* Procedimientos de auditoría de seguridad de las PCI DSS versión 1.1. *Para obtener la información completa, consulte* PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2 (Resumen de cambios de las Normas de seguridad de los datos de la PCI de la PCI DSS versión 1.1 a 1.2).	
Julio de 2009	*1.2.1*	*Agregar la oración que se eliminó incorrectamente entre la PCI DSS versión 1.1 y 1.2.*	*5*
		Corregir "then" por "than" en los procedimientos de prueba 6.3.7.a y 6.3.7.b.	*32*
		Eliminar la marca gris para las columnas "Implementado" y "No implementado" en el procedimiento de prueba 6.5.b.	*33*
		Para la Hoja de trabajo de controles de compensación - Ejemplo completo, corregir la redacción al principio de la página por "Utilizar esta hoja de trabajo para definir los controles de compensación para cualquier requisito indicado como 'implementado' a través de los controles de compensación".	*64*

Índice

Introducción y descripción general de las normas de seguridad de datos de la PCI

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Este documento, *Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad,* utiliza como base los 12 requisitos de las DSS de la PCI y los combina con los procedimientos de evaluación pertinentes en una herramienta de evaluación de seguridad. Se diseñó para que lo utilizaran los asesores que realizan visitas en el sitio del comerciante y de los proveedores de servicios que deben validar la conformidad con las DSS de la PCI. A continuación, encontrará una descripción general de los 12 requisitos de las DSS de la PCI. En las próximas páginas, encontrará información sobre la preparación, la conducción y el informe de una evaluación de las DSS de la PCI. La descripción detallada de los requisitos de las DSS de la PCI comienza en la página 13.

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Crear y mantener una red segura	
Requisito 1:	Instale y mantenga una configuración de firewall para proteger los datos de los titulares de las tarjetas
Requisito 2:	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteja los datos del titular de la tarjeta	
Requisito 3:	Proteja los datos del titular de la tarjeta que fueron almacenados
Requisito 4:	Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas
Desarrolle un programa de administración de vulnerabilidad	
Requisito 5:	Utilice un software antivirus y actualícelo regularmente
Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras
Implemente medidas sólidas de control de acceso	
Requisito 7:	Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa
Requisito 8:	Asigne una ID exclusiva para cada persona que tenga acceso al sistema informático
Requisito 9:	Limite el acceso físico a los datos del titular de la tarjeta
Supervise y pruebe las redes regularmente	
Requisito 10:	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas
Requisito 11:	Pruebe los sistemas y procesos de seguridad regularmente
Mantenga una política de seguridad de información	
Requisito 12:	Mantenga una política que aborde la seguridad de la información

Información sobre la aplicabilidad de las DSS de la PCI

La siguiente tabla ilustra los elementos de los datos de titulares de tarjetas y los datos confidenciales de autenticación que habitualmente se utilizan; independientemente de que esté permitido o prohibido el almacenamiento de dichos datos o de que esos datos deban estar protegidos. Esta tabla no es exhaustiva, sino que tiene por objeto ilustrar distintos tipos de requisitos que se le aplican a cada elemento de datos.

Los requisitos de las PCI DSS se aplican si se almacena, procesa o transmite un Número de cuenta principal (PAN). Si un PAN no se almacena, procesa ni transmite, no se aplican los requisitos de las PCI DSS.

	Elemento de datos	Almacenamiento permitido	Protección requerida	PCI DSS req. 3.4
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí	Sí
	Nombre del titular de la tarjeta [1]	Sí	Sí [1]	No
	Código de servicio [1]	Sí	Sí [1]	No
	Fecha de vencimiento [1]	Sí	Sí [1]	No
Datos confidenciales de autenticación [2]	Datos completos de la banda magnética [3]	No	N/C	N/C
	CAV2/CVC2/CVV2/CID	No	N/C	N/C
	PIN/Bloqueo de PIN	No	N/C	N/C

1 *Estos elementos de datos deben quedar protegidos si se los almacena con el PAN. Esta protección debe brindarse por cada requisito de las DSS de la PCI, a fin de asegurar una protección integral del entorno de los datos del titular de la tarjeta. Además, es posible que otras leyes (por ejemplo, las leyes relacionadas con la protección, la privacidad, el robo de identidad o la seguridad de los datos personales del consumidor) exijan protección específica de esos datos o la debida divulgación de las prácticas de una empresa en caso de que se recopilen datos personales sobre el consumidor durante el transcurso de los negocios. Sin embargo, las DSS de la PCI no rigen si no se almacenan, procesan ni transmiten los PAN.*

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

3 *Contenido completo de la pista de banda magnética, imagen de la banda magnética que está en el chip o en cualquier otro dispositivo.*

Alcance de la evaluación del cumplimiento de los requisitos de las DSS de la PCI

Los requisitos de seguridad de las DSS de la PCI rigen para todos los componentes del sistema. Los “componentes del sistema” se definen como todo componente de la red, del servidor o de la aplicación que se incluye en el entorno de los datos del titular de la tarjeta o que está conectado a éste. El entorno de los datos del titular de la tarjeta es la parte de la red que posee los datos del titular de la tarjeta o los datos confidenciales de autenticación. Los componentes de la red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de la red y otras aplicaciones de seguridad. Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, base de datos, autenticación, correo electrónico, proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS). Las aplicaciones incluyen todas las aplicaciones compradas y ordinarias, incluidas las aplicaciones internas y externas (Internet).

Segmentación de red

La segmentación de red, o separación (segmentación), del entorno de los datos del titular de la tarjeta del resto de la red corporativa no constituye un requisito de las DSS de la PCI. Sin embargo, se recomienda como método que puede disminuir:

- El alcance de la evaluación de las DSS de la PCI.
- El costo de la evaluación de las DSS de la PCI.
- El costo y la dificultad de la implementación y del mantenimiento de los controles de las DSS de la PCI.
- El riesgo de las organizaciones (que, gracias a la consolidación de los datos del titular de la tarjeta en menos y más controladas ubicaciones, se ve reducido)

Sin la adecuada segmentación de red (a veces denominada "red simple"), toda la red se encuentra dentro del alcance de la evaluación de las DSS de la PCI. La segmentación de red se puede alcanzar mediante firewalls internos de red, routers con sólidas listas de control de acceso u otra tecnología que restringe el acceso a un segmento particular de la red.

Un prerequisito importante para reducir el alcance del entorno de los datos del titular de la tarjeta es la comprensión de las necesidades de la empresa y de los procesos relacionados con el almacenamiento, el procesamiento y la transferencia de los datos del titular de la tarjeta. Es posible que la restricción de los datos del titular de la tarjeta a la menor cantidad posible de ubicaciones mediante la eliminación de datos innecesarios y la consolidación de datos necesarios necesite la reingeniería de prácticas empresariales de larga data.

La documentación de los flujos de datos del titular de la tarjeta mediante un diagrama de flujo de datos ayuda a comprender completamente todos los flujos de datos del titular de la tarjeta y a asegurar que toda segmentación de red logre aislar el entorno de los datos del titular de la tarjeta.

Si existe una segmentación de red implementada que se utilizará para disminuir el alcance de la evaluación de las DSS de la PCI, el asesor debe controlar que la segmentación pueda reducir el alcance de la evaluación. De la manera más detallada posible, la adecuada segmentación de red aísla los sistemas que almacenan, procesan o transfieren datos del titular de la tarjeta de los sistemas que no realizan estas operaciones. Sin embargo, la aptitud de la implementación de una segmentación de red en particular varía y depende de ciertas cuestiones como la configuración de determinadas redes, las tecnologías que se utilizan y los otros controles que puedan implementarse.

Anexo F: Las revisiones de las DSS de la PCI – Alcance y selección de muestras proporcionan más información del efecto del alcance durante la evaluación de las DSS de la PCI

Medios inalámbricos

Si se utiliza tecnología inalámbrica para almacenar, procesar o transferir datos del titular de la tarjeta (por ejemplo, transacciones de puntos de venta, “line-busting”) o si hay una red de acceso local (LAN) inalámbrica conectada al entorno de datos de los titulares de la tarjeta o a una parte del mismo (por ejemplo, que no esté claramente separada por el firewall), se aplican y se deben implementar los requisitos y procedimientos de evaluación para entornos inalámbricos de las DSS de la PCI (por ejemplo, requisitos 1.2.3, 2.1.1 y 4.1.1). Recomendamos que antes de implementar la tecnología inalámbrica, la empresa debe evaluar cuidadosamente la necesidad de contar con esta tecnología tomando en cuenta el riesgo. Tenga en cuenta la implementación de la tecnología inalámbrica solamente para las transmisiones de datos no confidenciales.

Terceros/terciarización

En el caso de proveedores de servicios que deben realizar una evaluación anual en el sitio, la validación de cumplimiento se debe realizar en todos los componentes del sistema en los que se almacenan, procesan o transfieren datos del titular de la tarjeta.

Los comerciantes o proveedores de servicio pueden utilizar terceros para almacenar, procesar y transferir datos del titular de la tarjeta en su nombre o para administrar componentes como routers, firewalls, bases de datos, seguridad física o servidores. En ese caso, la seguridad del entorno de los datos del titular de la tarjeta podría estar afectada.

En el caso de las entidades que terciarizan el almacenamiento, el procesamiento o la transferencia de datos del titular de la tarjeta a terceros proveedores de servicios, el Informe de cumplimiento (ROC) debe documentar el rol que desempeña cada proveedor de servicio e identificar claramente los requisitos que se aplican a la entidad evaluada y los que se aplican al proveedor de servicios. Los terceros proveedores de servicios tienen dos formas de validar el cumplimiento: 1) Pueden realizar una evaluación de las DSS de la PCI por su cuenta y proporcionar pruebas a sus clientes a los efectos de demostrar su cumplimiento o 2) en el caso de que no realicen la evaluación de las DSS de la PCI por su cuenta, sus servicios se evaluarán durante el transcurso de las evaluaciones de las DSS de la PCI de cada uno de sus clientes. Para obtener más información, consulte el punto que comienza con "En el caso de revisiones administradas de proveedores de servicios (MSP)" en la Parte 3 de la sección "Instrucciones y contenido del informe de cumplimiento".

Asimismo, los comerciantes y los proveedores de servicios deben administrar y supervisar el cumplimiento de las DSS de la PCI de los terceros relacionados que tengan acceso a los datos del titular de la tarjeta. *Consulte el Requisito 12.8 de este documento para obtener información más detallada.*

Control de las instalaciones de la empresa y de los componentes del sistema

El asesor puede seleccionar muestras representativas de las instalaciones de la empresa y de los componentes del sistema para evaluar los requisitos de las DSS de la PCI. Estas muestras deben incluir tanto componentes del sistema como instalaciones de la empresa. Las muestras deben ser una selección representativa de todos los tipos y de todas las ubicaciones de las instalaciones de la empresa como también de todos los componentes del sistema. La muestra debe ser lo suficientemente grande como para asegurarle al asesor que los controles se hayan implementado de la manera esperada.

Las oficinas corporativas, los comercios, las franquicias y las instalaciones de las empresas en distintas ubicaciones son ejemplos de instalaciones. Las muestras deben incluir componentes de sistemas de cada instalación de la empresa. Por ejemplo, por cada instalación de la empresa, incluya distintos sistemas operativos, funciones y aplicaciones que se utilizan en el área en evaluación. Por ejemplo, en cada instalación de la empresa, el asesor podría elegir los servidores Sun que operan con Apache WWW, los servidores Windows que operan con Oracle, los sistemas mainframe que operan con aplicaciones heredadas de procesamiento de tarjetas, los servidores de transferencia de datos que operan con HP-UX y servidores Linux que operan con MYQL. Si todas las aplicaciones operan desde un mismo sistema operativo (por ejemplo, Windows o Sun), la muestra deberá incluir una variedad de aplicaciones (por ejemplo, servidores de base de datos, servidores de Web y servidores de transferencia de datos, etc.). (*Consulte el Anexo F: Revisiones de las DSS de la PCI: alcance y control*).

Al seleccionar muestras de las instalaciones de la empresa y de los componentes del sistema, los asesores deberán tener en cuenta lo siguiente:

- Si existen procesos estándares necesarios de las DSS de la PCI que cada instalación debe cumplir, la muestra puede ser menor de lo que sería necesario si no existieran procesos estándares, a fin de asegurar que cada instalación está configurada de acuerdo con el proceso estándar.
- Si existiera más de un tipo de proceso estándar implementado (por ejemplo, para diferentes tipos de componentes del sistema o de instalaciones), la muestra debe ser lo suficientemente grande como para incluir los componentes del sistema y las instalaciones aseguradas con cada tipo de proceso.
- Si no hay procesos estándares de las DSS de la PCI implementados y cada instalación es responsable por sus propios procesos, el tamaño de la muestra debe ser mayor para tener la certeza de que cada instalación entiende e implementa en forma apropiada los requisitos de las DSS de la PCI.

Consulte el Anexo F: Revisiones de las DSS de la PCI: control de alcance y de selección de muestras.

Controles de compensación

Anualmente, el asesor deberá documentar, revisar y validar los controles de compensación e incluirlos con el Informe de cumplimiento que presente, según se ilustra en el *Anexo B. Controles de compensación* y *Anexo C: Hoja de trabajo de controles de compensación.*

Por cada control de compensación, se **debe** completar la Hoja de trabajo de controles de compensación (Anexo C). Asimismo, los controles de compensación se deben documentar en el ROC en la sección de los requisitos pertinentes de las DSS de la PCI.

Para obtener más información sobre “controles de compensación”, consulte los Anexos B y C nombrados anteriormente.

Instrucciones y contenido del informe de cumplimiento

Este documento se debe utilizar como modelo para crear el *Informe de cumplimiento*. La entidad que se evalúe deberá seguir los requisitos de informe de cada marca de pago para asegurar que cada marca de pago reconozca el estado de cumplimiento de la entidad. Comuníquese con cada marca de pago para establecer los requisitos e instrucciones de informe.

Contenido y formato del informe

Siga estas instrucciones relacionadas con el contenido y con el formato del informe al completar un Informe de cumplimiento:

1. Resumen ejecutivo

Incluya lo siguiente:

- Describa el negocio de tarjeta de pago de la entidad, incluya:
  - El papel de su empresa con las tarjetas de pago, que es la manera en la que almacenan, procesan o transfieren los datos del titular de la tarjeta y la razón por la cual lo hacen.

    Nota: Esto no debe ser un cortar y pegar del sitio web de la entidad, pero debe ser una descripción adaptada que muestre que el asesor comprende el pago y el papel de la entidad.
  - Forma en que procesan el pago (directamente, indirectamente, etcétera)
  - Los tipos de canales de pago a los que prestan servicios, como transacciones con tarjeta ausente (por ejemplo, pedido por correo-pedido por teléfono [MOTO], comercio electrónico) o transacciones con tarjeta presente.
  - Toda entidad a la que se conectan para la transmisión o para el procesamiento de pagos, incluidas las relaciones de procesador.
- Un diagrama de la red muy detallado (ya sea proporcionado por la entidad o creado por el asesor) de la topografía de la red de la entidad que incluya:
  - Conexiones hacia y desde la red
  - Los componentes importantes que hay dentro del entorno de datos del titular de la tarjeta, incluidos los dispositivos POS, los sistemas, las bases de datos y los servidores web según corresponda.
  - Otros componentes de pago necesarios, según corresponda.

2. Descripción del alcance del trabajo y del enfoque adoptado

Describa el alcance, conforme al Alcance de la evaluación de este documento, e incluya lo siguiente:

- Entorno en el cual se centró la evaluación (por ejemplo, puntos de acceso a Internet del cliente, red corporativa interna, conexiones de procesamiento)
- En el caso de que se implemente la segmentación de red y se utilice para disminuir el alcance de la revisión de las DSS de la PCI, describa esa segmentación y la manera en la que el asesor validó la eficacia de la segmentación.
- Documente y justifique las muestras utilizadas tanto en las entidades (comercios, instalaciones, etc.) como en los componentes del sistema que se eligieron, incluya:
  - Población total
  - Cantidad de muestras
  - Base para la selección de muestras
  - La razón por la cual el tamaño de la muestra es suficiente para que el asesor confíe en que los controles evaluados reflejan los controles implementados en toda la entidad.
  - Describa toda ubicación o entorno que almacene, procese o transfiera datos de titulares de tarjetas que se EXCLUYERON del alcance de la revisión y la razón por la que se excluyeron.
- Enumere toda entidad en propiedad absoluta que requiera cumplimiento con las DSS de la PCI y aclare si se evalúa por separado o como parte de esta evaluación.
- Enumere toda entidad internacional que requiera cumplimiento con las DSS de la PCI y aclare si se evalúa por separado o como parte de esta evaluación.
- Enumere toda LAN inalámbrica o aplicación inalámbrica de pago (por ejemplo, terminales POS) que esté conectada al entorno de datos del titular de la tarjeta o que pueda tener efectos sobre su seguridad y describa las medidas de seguridad implementadas para estos entornos inalámbricos.
- La versión del documento Procedimientos de evaluación de seguridad y requisitos de las DSS de la PCI utilizado para realizar la evaluación.
- Plazo de la evaluación

3. Información sobre el entorno evaluado

Incluya la siguiente información en esta sección:

- Un diagrama de cada pieza del vínculo de comunicación, que incluya LAN, WAN o Internet
- Descripción del entorno de datos del titular de la tarjeta, por ejemplo:
  - Transmisión de documentos y procesamiento de datos de titulares de tarjetas, incluida la autorización, la captura, la liquidación y los flujos de reintegros de cobros, según corresponda.

  - Lista de los archivos y las tablas que almacenan datos de titulares de tarjetas, respaldados por un inventario creado (u obtenido del proveedor de software) y retenido por el asesor en los documentos de trabajo. Para cada almacenamiento (archivo, tabla, etc.) de datos de titulares de tarjetas, este inventario debe incluir:
    - Una lista de todos los elementos correspondientes a los datos almacenados de los titulares de tarjetas.
    - Cómo se aseguran los datos.
    - Cómo se registra el acceso al almacenamiento de datos.
- Lista de hardware y de software importante que se utiliza en el entorno de los datos de titulares de tarjetas junto con una descripción de la función/uso de cada uno.
- Lista de proveedores de servicios y de otras entidades con las cuales la empresa comparte datos de titulares de tarjetas (Nota: estas entidades están sujetas al Requisito 12.8 de las DSS de la PCI).
- Lista de productos de aplicación de pago de terceros y números de las versiones que se utilizan, incluyendo si cada aplicación de pago se validó conforme a PA-DSS. Incluso si una aplicación de pago se validó conforme a PA-DSS, el asesor debe controlar que la aplicación se implementó de forma tal y en un entorno que cumple con las DSS de la PCI y conforme a la Guía de implementación de PA-DSS del vendedor de la aplicación de pago. Nota: La utilización de aplicaciones PA-DSS validadas no es requisito de las DSS de la PCI. Consulte a cada marca de pago por separado para comprender sus requisitos de cumplimiento de PA-DSS.
- Lista de las personas consultadas y sus cargos
- Lista de la documentación revisada
- En el caso de las revisiones de proveedores de servicio administrados (MSP), el asesor debe detallar claramente los requisitos de este documento que se aplican a los MSP (y que se incluyen en la revisión) y los que no se incluyen en la revisión que los clientes de los MSP deben incluir en sus propias revisiones. Incluya información sobre cuáles direcciones IP de MSP se analizan como parte de los análisis de vulnerabilidad trimestrales de los MSP y cuáles direcciones IP los clientes de los MSP deben incluir en sus propios análisis trimestrales.

4. Información de contacto y fecha del informe

Incluya:

- La información de contacto del comerciante o del proveedor de servicio y del asesor.
- Fecha del informe

5. Resultados del análisis trimestral

- Resuma los resultados de los últimos cuatro análisis trimestrales en el Resumen ejecutivo como también en los comentarios del Requisito 11.2.

Nota: No es necesario que transcurran cuatro análisis trimestrales aprobados para el cumplimiento de las DSS de la PCI inicial si el asesor verifica que 1) el último resultado de análisis fue un análisis aprobado, 2) la entidad documentó políticas y procedimientos que necesitan que el análisis trimestral continúe y 3) toda deficiencia que se observó en el análisis inicial se corrigió como se muestra en el análisis que se volvió a realizar. En el caso de años siguientes a la revisión inicial de las DSS de la PCI, deben obtenerse cuatro análisis aprobados.

- El análisis debe incluir todas las direcciones IP a las cuales se puede acceder externamente (Internet) que existan en la entidad conforme a los *Procedimientos de análisis de seguridad de las DSS de la PCI*

6. Conclusiones y observaciones

- Sintetice en el Resumen ejecutivo todo hallazgo que no cumpla con el formato del Informe de cumplimiento estándar.
- Todos los asesores *deben* utilizar la plantilla Requisitos de las DSS de la PCI y procedimientos de evaluación de seguridad detallados a los efectos de brindar detalladas descripciones y conclusiones de informes sobre cada requisito y subrequisito.
- El asesor *debe* analizar y documentar todo control de compensación que se utiliza para sostener que se implementan determinados controles.

  Para obtener más información sobre los "controles de compensación", consulte la sección Controles de compensación que aparece más arriba los Anexos B y C.

Revalidación de puntos sujetos a control

A los efectos de verificar el cumplimiento, se necesita un informe de "controles implementados". Este informe se interpretará como incumplidor si existieran "puntos sujetos a control" o puntos que se terminarán en una fecha posterior. El comerciante/proveedor de servicios debe corregir estos puntos antes de que se complete la validación. Después de que el comerciante/proveedor de servicios corrigió estos puntos, el asesor volverá a evaluarlos a los efectos de validar que se realizó la corrección y que se cumplieron todos los requisitos. Con posterioridad a la revalidación, el asesor confeccionará un nuevo Informe de cumplimiento en el que verificará que el entorno de los datos del titular de la tarjeta se encuentra en cumplimiento y lo presentará conforme a las instrucciones (vea más abajo).

Cumplimiento de las DSS de la PCI: pasos de cumplimiento

1. Complete el Informe de cumplimiento (ROC) conforme a la sección anterior "Instrucciones y contenido del informe de validación".
2. Asegúrese de que un Proveedor Aprobado de Escaneo (ASV) de las DSS de la PCI completó los análisis aprobados de vulnerabilidad y solicítele pruebas al ASV de los análisis aprobados.
3. Complete la Declaración de cumplimiento en su totalidad, ya sea para Proveedores de servicios o Comerciantes. Para obtener información sobre la declaración, consulte los Anexos D y E.
4. Presente el ROC, las pruebas del análisis aprobado y la Declaración de cumplimiento junto con todo otro documento solicitado al adquirente (en el caso de comerciantes), a la marca de pago o a todo otro solicitante (en el caso de proveedores de servicios).

Requisitos de las DSS de la PCI y procedimientos de evaluación de seguridad detallados

En el caso de los *Requisitos de las DSS de la PCI y procedimientos de evaluación de seguridad* lo que se detalla a continuación define los encabezados de las columnas de la tabla:

- **Requisitos de las DSS de la PCI:** esta columna define las normas de seguridad de datos y enumera los requisitos para alcanzar el cumplimiento de las DSS de la PCI, el cumplimiento se validará en comparación con estos requisitos.
- **Procedimientos de evaluación:** esta columna muestra los procesos que el asesor debe seguir a los efectos de validar que los requisitos de las DSS de la PCI "se hayan implementado".
- **Implementado:** el asesor debe utilizar esta columna a los efectos de proporcionar una breve descripción de los controles que encontró implementados, incluidos aquellos controles que están implementados gracias a los controles de compensación. (Nota: esta columna *no* debe utilizase en el caso de puntos que todavía no se implementaron o en el caso de puntos que se completarán en el futuro.)
- **No implementados:** el asesor debe utilizar esta columna a los efectos de proporcionar una breve descripción de los controles que no están implementados. Cabe destacar que un informe en incumplimiento no se debe presentar ante la marca de pago o ante el adquirente salvo que se solicite especialmente. Consulte los Anexos D y E: Declaración de cumplimiento para obtener instrucciones adicionales relativas a informes en incumplimiento.
- **Fecha objetivo/comentarios:** en el caso de los controles "No implementados", el asesor puede incluir una fecha programada en la que el comerciante o el proveedor de servicios proyecta "Implementar" los controles. Toda anotación u observación, también, se puede incluir en esta columna.

Desarrollar y mantener una red segura

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas

Los firewalls son dispositivos computarizados que controlan el tránsito permitido en la red de una empresa (interna) y de redes no confiables (externas) así como el tránsito de entrada y salida a áreas más sensibles dentro de la red interna confidencial de la empresa. El entorno del titular de la tarjeta es un ejemplo de un área más confidencial dentro de la red confiable de la empresa.

El firewall evalúa todo el tránsito de la red y bloquea las transmisiones que no cumplen con los criterios especificados de seguridad.

Es necesario proteger todos los sistemas contra el acceso no autorizado desde redes no confiables, ya sea que ingresen al sistema a través de Internet como comercio electrónico, del acceso a Internet desde las computadoras de mesa de los empleados, del acceso al correo electrónico de los empleados, de conexiones dedicadas como conexiones de empresa a empresa mediante redes inalámbricas o a través de otras fuentes. Con frecuencia, algunas vías de conexión hacia y desde redes no confiables aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los firewalls son un mecanismo de protección esencial para cualquier red de computadores.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.1 Establezca los estándares de configuración del firewall y del router que incluyen lo siguiente:	**1.1** Obtenga e inspeccione los estándares de configuración del firewall y del router y otros documentos enumerados más abajo para verificar que los estándares se completaron. Complete lo siguiente:			
1.1.1 Un proceso formal para aprobar y evaluar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers	**1.1.1** Controle la existencia de un proceso formal para aprobar y evaluar todos los cambios y las conexiones de red en la configuración de los firewalls y de los routers.			
1.1.2 Un diagrama actualizado de la red con todas las conexiones que acceden a los datos de los titulares de las tarjetas, incluida toda red inalámbrica	**1.1.2.a** Controle que exista un diagrama actualizado de la red (por ejemplo, uno que muestre los flujos de los datos de los titulares de la tarjeta en la red) que documenta todas las conexiones a los datos de los titulares de las tarjetas, incluida toda red inalámbrica.			
	1.1.2.b Controle que el diagrama se mantenga al día.			
1.1.3 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de la red interna	**1.1.3** Controle que los estándares de configuración del firewall incluyan requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ y la zona de la red interna. Controle que el diagrama actual de la red concuerde con los estándares de configuración de firewalls.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.1.4 Descripción de grupos, de papeles y de responsabilidades para una administración lógica de los componentes de la red	**1.1.4** Controle que los estándares de configuración del firewall y el router incluyan la descripción de grupos, de papeles y de responsabilidades para una administración lógica de los componentes de la red.			
1.1.5 Razón documentada y comercial para la utilización de todos los servicios, los protocolos y los puertos permitidos, incluida la documentación de funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros	**1.1.5.a** Controle que los estándares de configuración de firewalls y de routers incluyan una lista documentada de los servicios, de los protocolos y de los puertos necesarios para las operaciones, por ejemplo, el protocolo de transferencia de hipertexto (HTTP) y los protocolos Protocolo de Capa de Conexión Segura (SSL), Secure Shell (SSH) y Red Privada Virtual (VPN).			
	1.1.5.b Identifique servicios, protocolos y puertos inseguros permitidos y controle que sean necesarios y que las funciones de seguridad se documenten e implementen mediante la evaluación de los estándares de configuración del firewall y del router y de los ajustes de cada servicio. Un ejemplo de un servicio, protocolo o puerto inseguro es FTP, que transfiere las credenciales del usuario en textos claros.			
1.1.6 Requisito de la revisión de las normas del firewall y el router, al menos, cada seis meses.	**1.1.6.a** Controle que los estándares de configuración del firewall y el router soliciten la revisión de las normas de éstos al menos cada seis meses.			
	1.1.6.b Obtenga y examine la documentación a los efectos de verificar que los conjuntos de normas se revisen al menos cada seis meses.			
1.2 Desarrolle una configuración de firewall que restrinja las conexiones entre redes no confiables y todo componente del sistema en el entorno de los datos del titular de la tarjeta.	**1.2** Evalúe la configuración de los firewalls y del router a los efectos de controlar que las conexiones entre redes no confiables y todo componente del sistema en el entorno de los datos del titular de la tarjeta se restringen de la siguiente manera:			
Nota: Una red "no confiable" es toda red que es externa a las redes que pertenecen a la entidad en evaluación y que excede la capacidad de control o administración de la entidad.				

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.2.1 Restrinja el tránsito entrante y saliente a la cantidad que sea necesaria en el entorno de datos del titular de la tarjeta.	**1.2.1.a** Controle que el tránsito entrante y saliente se restrinja a la cantidad que sea necesaria en el entorno de datos del titular de la tarjeta y que se documentan las restricciones.			
	1.2.1.b Controle que todo otro tránsito entrante o saliente se niegue, por ejemplo, mediante la utilización de una declaración explícita "negar todos" o una negación implícita después de una declaración de permiso.			
1.2.2 Asegure y sincronice los archivos de configuración de routers.	**1.2.2** Controle que los archivos de configuración de router sean seguros y se encuentren sincronizados, por ejemplo, los archivos de configuración en operación (utilizados para las operaciones normales de los routers) y los archivos de configuración de arranque (utilizados cuando las máquinas se reinician) tienen las mismas configuraciones de seguridad.			
1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar y controlar (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde el entorno inalámbrico hacia el entorno del titular de la tarjeta.	**1.2.3** Controle la existencia de firewalls de perímetro instalados entre las redes inalámbricas y los sistemas que almacenan datos de titulares de tarjetas y que estos firewalls niegan y controlan (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde el entorno inalámbrico hacia el entorno del titular de la tarjeta.			
1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.	**1.3** Evalúe las configuraciones de los firewalls y routers, de la manera que se describe más abajo, a los efectos de establecer que no existe acceso directo entre Internet y los componentes del sistema, incluido el router de estrangulamiento de Internet, el router DMZ y el firewall, el segmento de titulares de tarjeta de DMZ, el router de perímetro y el segmento de la red interna del titular de la tarjeta.			
1.3.1 Implemente un DMZ para limitar el tránsito entrante y saliente a los protocolos que sean necesarios en el entorno de datos del titular de la tarjeta.	**1.3.1** Controle que se haya implementado un DMZ para limitar el tránsito entrante y saliente a los protocolos que sean necesarios en el entorno de datos del titular de la tarjeta.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.3.2 Restrinja el tránsito entrante de Internet a las direcciones IP dentro del DMZ.	**1.3.2** Controle que se restrinja el tránsito entrante de Internet a las direcciones IP dentro del DMZ.			
1.3.3 No permita ninguna ruta directa de entrada o salida de tránsito entre Internet y el entorno del titular de la tarjeta.	**1.3.3** Controle que no exista ninguna ruta directa de entrada o salida de tránsito entre Internet y el entorno del titular de la tarjeta.			
1.3.4 No permita que las direcciones internas pasen desde Internet al DMZ.	**1.3.4** Controle que las direcciones internas no puedan pasar desde Internet al DMZ**.**			
1.3.5 Restrinja el tránsito saliente del entorno de datos del titular de la tarjeta a Internet de forma tal que el tránsito saliente sólo pueda acceder a direcciones IP dentro del DMZ.	**1.3.5** Controle que el tránsito saliente del entorno de datos del titular de la tarjeta a Internet sólo pueda acceder a direcciones IP dentro del DMZ.			
1.3.6 Implemente la inspección completa, también conocida como filtrado dinámico de paquetes. (Es decir, sólo se permite la entrada a la red de conexiones “establecidas”).	**1.3.6** Controle que el firewall realice una inspección completa (filtro de paquete dinámico). [Sólo se deben permitir la entrada de conexiones establecidas y sólo si están asociadas con una sesión previamente establecida (ejecute un análisis de puertos en todos los puertos TCP con el conjunto de bits “syn reset” o ”syn ack”, una respuesta significa que se permite la entrada a paquetes aunque no formen parte de una sesión previamente establecida)].			
1.3.7 Coloque la base de datos en una zona de red interna, segregada del DMZ.	**1.3.7** Controle que la base de datos se encuentre en una zona de red interna, segregada del DMZ.			
1.3.8 Implemente la simulación IP a los efectos de evitar que las direcciones internas se traduzcan y se divulguen en Internet mediante la utilización del espacio de dirección RFC 1918. Utilice tecnologías de traducción de dirección de red (NAT), por ejemplo traducción de dirección de puertos (PAT).	**1.3.8** En la muestra de componentes de firewalls y routers, controle que se use la tecnología NAT u otra tecnología que utilice el espacio de dirección RFC 1918 para restringir las transmisiones de direcciones IP desde la red interna hacia Internet (simulación IP).			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.4 Instale software de firewall personal en toda computadora móvil o de propiedad de los trabajadores con conectividad directa a Internet (por ejemplo, laptops que usan los trabajadores), mediante las cuales se accede a la red de la organización.	**1.4.a** Controle que toda computadora móvil o de propiedad de los trabajadores con conectividad directa a Internet (por ejemplo, laptops que usan los trabajadores) que se utilice para acceder a la red de la organización posea software de firewall personal instalado y activo.			
	1.4.b Controle que la organización configure el software de firewall personal a los efectos de detallar los estándares y que no se pueda alterar por usuarios de computadoras móviles.			

Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

Los delincuentes (externos e internos a la empresa), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para afectar los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se establecen fácilmente por medio de información pública.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
2.1 Siempre cambie los valores predeterminados de los proveedores **antes** de instalar un sistema en la red (por ejemplo, incluya contraseñas, cadenas comunitarias de protocolo simple de administración de red [SNMP] y elimine cuentas innecesarias).	**2.1** Elija una muestra de componentes de sistemas e intente conectarse (con ayuda del administrador del sistema) a los dispositivos que usan las cuentas y contraseñas proporcionadas por los proveedores a los efectos de controlar que las cuentas y las contraseñas predeterminadas se cambiaron. (Utilice los manuales y fuentes de los proveedores de Internet para encontrar las cuentas y contraseñas proporcionadas por éstos).			
2.1.1 En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transfieren datos del titular de la tarjeta, cambie los valores predeterminados proporcionados por los proveedores, incluidos, a modo de ejemplo, claves de criptografía inalámbricas predeterminadas, contraseñas y cadenas comunitarias SNMP. Asegúrese de que la configuración de seguridad de los dispositivos inalámbricos esté habilitada para la tecnología de cifrado de la autenticación y transmisión.	**2.1.1** Controle lo siguiente con respecto a los valores predeterminados proporcionados por los proveedores en los entornos inalámbricos y asegúrese de que todas las redes inalámbricas implementan sólidos mecanismos de cifrado (por ejemplo, AES): ▪ Las claves de cifrado predeterminadas se cambiaron al momento de su instalación y se cambian cada vez que una persona que tenga conocimiento de éstas cesa en sus funciones o se traslada a otro cargo en la empresa ▪ Se cambiaron las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos ▪ Se cambiaron las contraseñas predeterminadas de los puntos de acceso ▪ El firmware de los dispositivos inalámbricos se actualiza a los efectos de admitir el cifrado sólido para la autenticación y la transmisión en redes inalámbricas (por ejemplo, WPA/WPA2) ▪ Otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria.	**2.2.a** Evalúe las normas de configuración de sistema de la organización para todos los tipos de componentes de sistema y controle que las normas de configuración de sistema concuerden con las normas de alta seguridad aceptadas en la industria, por ejemplo, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) y Center for Internet Security (CIS).			
	2.2.b Controle que las normas de configuración de sistema incluyan cada punto que aparece a continuación (2.2.1 – 2.2.4)			
	2.2.c Controle que las normas de configuración de sistema se apliquen al configurar nuevos sistemas.			
2.2.1 Implemente solamente una función principal por cada servidor.	**2.2.1** En el caso de la muestra de componentes del sistema, controle que sólo una función principal se haya implementado en cada servidor. Por ejemplo, los servidores web y DNS se deben implementar en servidores separados.			
2.2.2 Deshabilite todos los servicios y protocolos innecesarios e inseguros (servicios y protocolos que no sean directamente necesarios para desempeñar la función especificada de los dispositivos).	**2.2.2** En el caso de la muestra de componentes de sistema, controle los sistemas, servicios, daemons y protocolos habilitados. Controle que los servicios o protocolos innecesarios o inseguros no estén habilitados o estén justificados y documentados en cuanto al uso adecuado del servicio. Por ejemplo, FTP no se utiliza o se encripta por medio de SSH u otra tecnología.			
2.2.3 Configure los parámetros de seguridad del sistema para evitar el uso indebido.	**2.2.3.a** Consulte a los administradores de sistema y/o gerentes de seguridad para controlar que conocen las configuraciones comunes de parámetros de seguridad para los componentes de sistemas.			
	2.2.3.b Controle que las configuraciones comunes de parámetros de seguridad se incluyan en las normas de configuración del sistema.			
	2.2.3.c En el caso de la muestra de componentes del sistema, controle que los parámetros de seguridad se hayan configurado adecuadamente.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
2.2.4 Elimine todas las funcionalidades innecesarias, tales como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.	**2.2.4** En el caso de la muestra de componentes del sistema, controle que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios). Controle que las funciones habilitadas estén documentadas y admitan la configuración segura y que sólo la funcionalidad documentada se encuentre presente en las máquinas controladas.			
2.3 Cifre todo el acceso administrativo que no sea de consola. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y otros tipos de acceso administrativo que no sea de consola.	**2.3** En el caso ce la muestra de componentes del sistema, controle que el acceso administrativo que no sea de consola se cifre mediante: ▪ La observación de un administrador mientras se conecta a cada sistema a fin de controlar que se invoca un método sólido de cifrado antes de que se solicite la contraseña del administrador. ▪ El análisis de servicios y archivos de parámetros en los sistemas a fin de controlar que Telnet y otros comandos de conexión remota no están disponibles para uso interno y ▪ El control de que el acceso del administrador a la interfaz de administración basada en la web está cifrado mediante una sólida criptografía.			
2.4 Los proveedores de servicio de hospedaje deben proteger el entorno hosting y los datos del titular de la tarjeta. Estos proveedores deben cumplir requisitos específicos detallados en el *Anexo A: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting.*	**2.4** Realice los procedimientos de evaluación desde **A.1.1** hasta **A.1.4** que se describen en *Anexo A: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting* en lo que respecta a la evaluación de las DSS de la PCI de los proveedores de hosting compartido para controlar que estos proveedores protejan los datos y el entorno sujeto al hosting de las entidades (comerciantes y proveedores de servicios).			

Proteja los datos del titular de la tarjeta

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la refundición son importantes componentes de la protección de datos del titular de la tarjeta. Si un intruso viola otros controles de seguridad de red y obtiene acceso a los datos cifrados, sin las claves criptográficas adecuadas no podrá leer ni utilizar esos datos. Los otros métodos eficaces para proteger los datos almacenados deberían considerarse oportunidades para mitigar el riesgo posible. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos de los titulares de la tarjeta salvo que sea absolutamente necesario, truncar los datos de los titulares de la tarjeta si no se necesita el PAN completo y no enviar el PAN en correos electrónicos no cifrados.

Consulte el *Glosario de términos, abreviaturas y acrónimos de las DSS de la PCI* para obtener definiciones de "criptografía sólida" y otros términos de las DSS de la PCI.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.1 Almacene la menor cantidad de datos posibles del titular de la tarjeta. Desarrolle una política de retención y de disposición de datos. Reduzca la cantidad de datos almacenados y el tiempo de retención a los que sean necesarios para fines comerciales, legales o reglamentarios, según se documente en la política de retención de datos.	**3.1** Obtenga y evalúe las políticas y los procedimientos de la empresa relativos a la retención y a la disposición de datos y haga lo siguiente ▪ Controle que las políticas y procedimientos incluyan los requisitos legales, reglamentarios y comerciales relativos a la retención de los datos, incluidos los requisitos específicos para la retención de los datos de los titulares de las tarjetas (por ejemplo, es necesario guardar los datos de los titulares de las tarjetas durante X tiempo por Y razones comerciales). ▪ Controle que las políticas y procedimientos incluyan cláusulas para la disposición de los datos cuando ya no sean necesarios por razones legales, reglamentarias o comerciales, incluida la disposición de los datos de los titulares de la tarjeta. ▪ Controle que las políticas y procedimientos incluyan la cobertura de todo almacenamiento de datos de los titulares de las tarjetas. ▪ Controle que las políticas y los procedimientos incluyan un proceso programático (automático) para eliminar, al menos trimestralmente, los datos almacenados de los titulares de las tarjetas que hayan excedido los requisitos comerciales de retención o, de forma alternativa, los requisitos de una revisión, que se realiza. al menos, trimestralmente, para controlar que los datos almacenados de los titulares de las tarjetas no exceden los requisitos comerciales de retención.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3 establecidos a continuación.	**3.2** Si se reciben y borran datos de autenticación confidenciales, obtenga y revise los procesos de eliminación de datos, a fin de controlar que los datos son irrecuperables. Por cada tipo de dato de autenticación confidencial que aparece a continuación, realice los siguientes pasos:			
3.2.1 No almacene contenidos completos de ninguna pista de la banda magnética (que está en el reverso de la tarjeta, 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 tarjeta.* ▪ *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.* *Nota: Consulte* Glosario de términos, abreviaturas y acrónimos de las DSS de la PCI *para obtener más información.*	**3.2.1** En el caso de la muestra de componentes del sistema, evalúe lo siguiente y controle que el contenido completo de cualquier pista de la banda magnética en el reverso de la tarjeta no se almacene en ninguna circunstancia: ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.2.2 No almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes. *Nota: Consulte* Glosario de términos, abreviaturas y acrónimos de las DSS de la PCI *para obtener más información.*	**3.2.2** En el caso de la muestra de componentes del sistema, controle que el código o el valor de verificación de la tarjeta de tres dígitos o de cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no quede almacenado en ninguna circunstancia: ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos			
3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.	**3.2.3** En el caso de la muestra de componentes del sistema, evalúe lo siguiente y controle que los PIN y los bloqueos de PIN cifrados no se almacenen en ninguna circunstancia: ▪ Datos de transacciones entrantes ▪ Todos los registros (por ejemplo, transacciones, historiales, depuración, error) ▪ Archivos de historial ▪ Archivos de seguimiento ▪ Esquemas de bases de datos ▪ Contenidos de bases de datos			
3.3 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá). *Notas:* ▪ *Este requisito no se aplica a trabajadores y a otras partes que posean una necesidad comercial legítima de conocer el PAN completo.* ▪ *Este requisito no reemplaza los requisitos más estrictos que fueron implementados y que aparecen en los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]).*	**3.3** Obtenga y evalúe las políticas escritas y revise las vistas de PAN (por ejemplo, en la pantalla, en recibos en papel) a fin de controlar que los números de las cuentas principales (PAN) se ocultan al visualizar los datos de los titulares de las tarjetas, excepto en los casos en que existe una necesidad comercial legítima de visualizar el PAN completo.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.4 Haga que el PAN quede, como mínimo, ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles y en registros) utilizando cualquiera 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). ▪ Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas. La información de cuenta MÍNIMA que se debe dejar ilegible es el PAN. *Notas:* ▪ *Si por alguna razón, la empresa no puede hacer que el PAN sea ilegible, consulte el* Anexo B: Controles de compensación. ▪ *La "sólida criptografía" se define en el* Glosario de términos, abreviaturas y acrónimos de las DSS de la PCI.	**3.4.a** Obtenga y evalúe documentación relativa al sistema utilizado para proteger el PAN, incluidos, el proveedor, el tipo de sistema/proceso y los algoritmos de cifrado (si corresponde). Controle que el PAN sea ilegible mediante la utilización 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). ▪ Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas.			
	3.4.b Evalúe varias tablas o archivos de la muestra de repositorios de datos para controlar que el PAN sea ilegible (es decir, no esté almacenado en formato de texto claro).			
	3.4.c Evalúe la muestra de medios removibles (como cintas de respaldo) para controlar que el PAN sea ilegible.			
	3.4.d Evalúe la muestra de registros de auditoría para controlar que el PAN se sanea o elimina de los registros.			
3.4.1 Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Las claves de descifrado no deben estar vinculadas a cuentas de usuarios.	**3.4.1.a** Si se utiliza el cifrado en disco, controle que el acceso lógico a los sistemas de archivos cifrados se implemente por medio de un mecanismo separado del mecanismo de los sistemas operativos nativos (por ejemplo, sin utilizar bases de datos de cuentas locales).			
	3.4.1.b Controle que las claves criptográficas estén almacenadas en forma segura (por ejemplo, se almacenen en medios portátiles protegidos adecuadamente con controles sólidos de acceso).			
	3.4.1.c Controle que los datos de los titulares de las tarjetas almacenados en medios portátiles se cifren donde quiera que se almacenen. *Nota: El cifrado de disco frecuentemente no puede cifrar medios portátiles, por lo tanto, los datos almacenados en estos medios se deben cifrar separadamente.*			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.5 Proteja las claves criptográficas que se utilizan para cifrar los datos de los titulares de tarjetas contra su posible divulgación o uso indebido:	**3.5** Controle los procesos que se utilizan para proteger las claves utilizadas para cifrar los datos de los titulares de tarjetas contra su posible divulgación o uso indebido mediante las siguientes acciones:			
3.5.1 Restrinja el acceso a las claves criptográficas al número mínimo de custodios necesarios.	**3.5.1** Evalúe las listas de acceso de usuarios para controlar que el acceso a las claves se restrinja a pocos custodios.			
3.5.2 Guarde las claves criptográficas de forma segura en la menor cantidad de ubicaciones y formas posibles.	**3.5.2** Evalúe los archivos de configuración de sistemas para controlar que las claves se almacenan en formato cifrado y que las claves de cifrado de claves se almacenan separadas de la claves de cifrado de datos.			
3.6 Documente completamente e implemente todos los procesos y los procedimientos de gestión de claves de las claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas, incluido lo siguiente:	**3.6.a** Controle la existencia de procedimientos de gestión de claves de las claves que se utilizan para el cifrado de datos de titulares de tarjetas. *Nota: Varias normas de la industria relativas a la administración de claves están disponibles en distintos recursos incluido NIST, que puede encontrar en http://csrc.nist.gov.*			
	3.6.b En el caso de proveedores de servicios solamente: Si el proveedor de servicio comparte claves con sus clientes para la transmisión de datos de los titulares de las tarjetas, controle que ese proveedor de servicio le proporcione documentación a los clientes que incluya lineamientos sobre la forma en que pueden almacenar y cambiar, en forma segura, sus claves (utilizadas para transmitir datos entre el cliente y el proveedor de servicio).			
	3.6.c Evalúe los procedimientos de administración de claves y realice lo siguiente:			
3.6.1 Generación de claves criptográficas sólidas	**3.6.1** Controle que los procedimientos de administración de clave se hayan implementado para solicitar la generación de claves sólidas.			
3.6.2 Distribución segura de claves criptográficas	**3.6.2** Controle que los procedimientos de administración de clave se hayan implementado para solicitar la distribución de claves seguras.			
3.6.3 Almacenamiento seguro de claves criptográficas	**3.6.3** Controle que los procedimientos de administración de clave se hayan implementado para solicitar el almacenamiento de claves seguras.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.6.4 Cambios periódicos de claves criptográficas ▪ Según se considere necesario y lo recomiende la aplicación asociada (por ejemplo, volver a digitar las claves), preferentemente en forma automática ▪ Por lo menos, anualmente	**3.6.4** Controle que los procedimientos de administración de clave se hayan implementado para solicitar cambios periódicos de clave, por lo menos, anualmente.			
3.6.5 Destrucción o reemplazo de claves criptográficas antiguas o supuestamente en riesgo	**3.6.5.a** Controle que los procedimientos de administración de clave se hayan implementado para solicitar la destrucción de claves antiguas (por ejemplo: archivo, destrucción y revocación, según corresponda).			
	3.6.5.b Controle que los procedimientos de administración de clave se hayan implementado para solicitar el reemplazo de claves que se sepa o se sospeche estén en riesgo.			
3.6.6 Divida el conocimiento y la creación del control dual de claves criptográficas	**3.6.6** Controle que se hayan implementado procedimientos de administración de clave que soliciten la división del conocimiento y del control dual de claves (por ejemplo, de forma que se requiera a dos o tres personas, cada una de las cuales conozca solamente una parte de la clave, para reconstruir la clave completa).			
3.6.7 Prevención de sustitución no autorizada de claves criptográficas	**3.6.7** Controle que los procedimientos de administración de clave se hayan implementado para solicitar la prevención de sustitución no autorizada de claves.			
3.6.8 Requisito de que los custodios de claves criptográficas firmen un formulario en el que declaren que comprenden y aceptan su responsabilidad como custodios de las claves	**3.6.8** Controle que los procedimientos de administración de claves se hayan implementado para solicitar que los custodios de claves firmen un formulario en el que declaren que comprenden y aceptan su responsabilidad como custodios de las claves.			

Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

La información confidencial se debe codificar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación pueden ser los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
4.1 Utilice criptografía y protocolos de seguridad sólidos como SSL/TLS o IPSEC para salvaguardar los datos confidenciales de los titulares de las tarjetas durante su transmisión a través de redes públicas abiertas. *Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las DSS de la PCI son:* ▪ *Internet* ▪ *Tecnologías inalámbricas* ▪ *Sistema global de comunicaciones móviles (GSM) y* ▪ *Servicio de radio paquete general (GPRS)*	**4.1.a** Controle el uso de cifrado (por ejemplo SSL/TLS o IPSEC) siempre que se transmitan o reciban datos de los titulares de las tarjetas a través de redes públicas abiertas ▪ Controle que se use el cifrado sólido durante la transmisión de datos. ▪ En el caso de la implementación de SSL: – Controle que el servidor admita las últimas versiones de parches. – Controle que HTTPS aparezca como parte del URL (Universal Record Locator) del navegador. – Controle que ningún dato del titular de la tarjeta se solicite cuando HTTPS no aparece en el URL. ▪ Seleccione una muestra de transacciones a medida que se reciben y observe las transacciones que se llevan a cabo para controlar que los datos de los titulares de las tarjetas se cifran durante el tránsito. ▪ Controle que sólo se acepten claves/certificados SSL/TSL de confianza. ▪ Controle que se implemente la solidez de cifrado adecuada para la metodología que se utiliza. (Consulte las recomendaciones/mejores prácticas de los proveedores).			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
4.1.1 Asegúrese de que las redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta utilizan las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión. ▪ *En el caso de nuevas implementaciones inalámbricas, se prohíbe la implementación WEP después del 31 de marzo de 2009.* ▪ *En el caso de actuales implementaciones inalámbricas, se prohíbe la implementación WEP después del 30 de junio de 2010.*	**4.1.1** En el caso de redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta, controle que utilicen las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión.			
4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea o el chat).	**4.2.a** Controle que se utilice criptografía sólida cada vez que se envían datos de los titulares de las tarjetas a través de tecnologías de mensajería de usuario final.			
	4.2.b Controle la existencia de una política que establezca que los PNA no cifrados no se deben enviar por medio de tecnologías de mensajería de usuario final.			

Desarrolle un programa de administración de vulnerabilidad

Requisito 5: Utilice y actualice regularmente el software o los programas antivirus

El software malicioso, llamado "malware", incluidos los virus, los gusanos (worm) y los troyanos (Trojan), ingresa a la red durante muchas actividades comerciales aprobadas incluidos los correos electrónicos de los trabajadores y la utilización de Internet, de computadoras portátiles y de dispositivos de almacenamiento y explota las vulnerabilidades del sistema. El software antivirus deberá utilizarse en todos los sistemas que el malware, por lo general, afecta para proteger los sistemas contra las amenazas de software maliciosos actuales o que eventualmente se desarrollen.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
5.1 Implemente software antivirus en todos los sistemas comúnmente afectados por software malicioso (en especial, computadoras personales y servidores).	**5.1** En el caso de la muestra de componentes del sistema que incluya todos los tipos de sistemas operativos comúnmente afectados por software malicioso, controle que se haya implementado software antivirus si existe la correspondiente tecnología antivirus.			
5.1.1 Asegúrese de que todos los programas antivirus son capaces de detectar y eliminar todos los tipos conocidos de software malicioso y de proteger a los sistemas contra éstos.	**5.1.1** En el caso de la muestra de componentes del sistema, controle que todos los programas antivirus detecten y eliminen todo los tipos conocidos de software malicioso (por ejemplo, virus, troyanos, gusanos, spyware, adware y rootkit) y que protejan a los sistemas contra éstos.			
5.2 Asegúrese de que todos los mecanismos antivirus son actuales, están en funcionamiento y son capaces de generar registros de auditoría.	**5.2** Controle que todos los mecanismos antivirus sean actuales, estén en funcionamiento y sean capaces de generar registros al realizar lo siguiente:			
	5.2.a Obtenga y evalúe la política y controle que solicite la actualización del software antivirus y las definiciones.			
	5.2.b Controle que la instalación maestra del software esté habilitada para la actualización automática y los análisis periódicos.			
	5.2.c En el caso de la muestra de componentes del sistema que incluya todos los tipos de sistemas operativos comúnmente afectados por software malicioso, controle que las actualizaciones automáticas y los análisis periódicos estén habilitados.			
	5.2d En el caso de la muestra de componentes del sistema, controle que la generación de registro de software antivirus esté habilitada y que esos registros se almacenen conforme al Requisito 10.7 de las DSS de la PCI			

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas importantes deben poseer la última versión de los parches adecuados para estar protegidos contra la explotación de los datos de los titulares de las tarjetas y el riego que representan los delincuentes y el software malicioso.

Nota: Los parches de software adecuados son aquéllos que se evaluaron y probaron para confirmar que no crean conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por la institución, es posible evitar numerosas vulnerabilidades mediante la utilización de procesos estándares de desarrollo de sistemas y técnicas de codificación segura.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.1 Asegúrese de que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes proporcionados por los proveedores. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. *Nota: Las organizaciones pueden tener en cuenta la aplicación de un enfoque basado en el riesgo a los efectos de priorizar la instalación de parches. Por ejemplo, al priorizar infraestructura de importancia (por ejemplo, dispositivos y sistemas públicos, bases de datos) superiores a los dispositivos internos menos críticos a los efectos de asegurar que los dispositivos y los sistemas de alta prioridad se traten dentro del periodo de un mes y se traten dispositivos y sistemas menos críticos dentro de un periodo de tres meses.*	**6.1.a** En el caso de la muestra de componentes del sistema y del software relacionado, compare la lista de parches de seguridad instalados en cada sistema con la última lista de parches de seguridad proporcionados por el proveedor a los efectos de confirmar que los actuales parches proporcionados por los proveedores están instalados.			
	6.1.b Evalúe las políticas relacionadas con la instalación de parches de seguridad a fin de establecer que solicitan la instalación de todos los nuevos parches de seguridad relevantes dentro de un plazo de un mes.			
6.2 Establezca un proceso para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, suscríbase a los servicios de alerta disponibles de forma gratuita . a través de Internet). Actualice las normas de configuración conforme al Requisito 2.2 de las DSS de la PCI para subsanar cualquier otro problema de vulnerabilidad.	**6.2.a** Consulte al personal responsable para controlar que se implementan procesos para identificar nuevas vulnerabilidades de seguridad.			
	6.2.b Controle que los procesos para identificar nuevas vulnerabilidades de seguridad incluyan el uso de fuentes externas de información sobre vulnerabilidades de seguridad y la actualización de las normas de configuración de sistemas revisadas en el Requisito 2.2 a medida que se encuentren nuevos problemas de vulnerabilidad.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.3 Desarrolle aplicaciones de software conforme a las DSS de la PCI (por ejemplo, registro y autenticación seguros) sobre la base de las mejores prácticas de la industria e incorpore la seguridad de la información en todo el ciclo de desarrollo de software. Los procedimientos deben incluir lo siguiente:	**6.3.a** Obtenga los procesos de desarrollo del software escritos y examínelos para verificar que estén basados en las normas de la industria y que se considere la seguridad en todo su ciclo de vida y que se desarrollen las aplicaciones de software conforme a las DSS de la PCI.			
	6.3.b A partir de un examen de los procesos de desarrollo del software escritos, las entrevistas con los desarrolladores de software y la inspección de los datos relevantes (documentación de la configuración de la red, los datos de producción y prueba, etc.), verifique lo siguiente:			
6.3.1 Las pruebas de todos los parches de seguridad y la configuración del sistema y del software cambien antes de su despliegue, incluidas, entre otras, las pruebas de lo siguiente:	**6.3.1** Todos los cambios (incluidos los parches) se evalúan antes de ser implementados para producción.			
6.3.1.1 Validación de las entradas (para prevenir el lenguaje de comandos entre distintos sitios, los errores de inyección, la ejecución de archivos maliciosos, etc.)	**6.3.1.1** Validación de las entradas (para prevenir el lenguaje de comandos entre distintos sitios, los errores de inyección, la ejecución de archivos maliciosos, etc.)			
6.3.1.2 Validación de un correcto manejo de los errores	**6.3.1.2** Validación de un correcto manejo de los errores			
6.3.1.3 Validación del almacenamiento criptográfico seguro	**6.3.1.3** Validación del almacenamiento criptográfico seguro			
6.3.1.4 Validación de las comunicaciones seguras	**6.3.1.4** Validación de las comunicaciones seguras			
6.3.1.5 Validación de un correcto control del acceso basado en funciones (RBAC)	**6.3.1.5** Validación de un correcto control del acceso basado en funciones (RBAC)			
6.3.2 Desarrollo/prueba por separado y entornos de producción	**6.3.2** Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control del acceso para reforzar la separación.			
6.3.3 Separación de funciones entre desarrollo/prueba y entornos de producción	**6.3.3** Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción.			
6.3.4 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo	**6.3.4** Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo ni se desinfectan antes de ser utilizados.			
6.3.5 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción	**6.3.5** Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.3.6 Eliminación de las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes que las aplicaciones se activen o se pongan a disposición de los clientes	**6.3.6** Personalización de las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes de activar los sistemas de producción o de que se pongan a disposición de los clientes.			
6.3.7 Revisión del código personalizado antes del envío a producción o a los clientes a fin de identificar posibles vulnerabilidades de la codificación *Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema que el Requisito 6.3 de las DSS de la PCI exige. Las revisiones de los códigos se pueden realizar por terceros o personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales, si son públicas, a los efectos de tratar con las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las DSS de la PCI.*	**6.3.7.a** Obtenga y analice las políticas para confirmar que todos los cambios a los códigos de aplicaciones personalizadas de *aplicaciones internas* se deban revisar (ya sea mediante procesos manuales o automáticos) de la siguiente manera: ▪ Los cambios a los códigos se revisan por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas seguras de codificación. ▪ Las correcciones pertinentes se implementan antes de su lanzamiento. ▪ La gerencia revisa y aprueba los resultados de la revisión de códigos antes de su lanzamiento.			
	6.3.7.b Obtenga y analice las políticas para confirmar que todos los cambios a los códigos de aplicaciones personalizadas de *aplicaciones web* se deban revisar (ya sea mediante procesos manuales o automáticos) de la siguiente manera: ▪ Los cambios a los códigos se revisan por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas seguras de codificación. ▪ Las revisiones de los códigos aseguran que los códigos se desarrollen conforme a lineamientos de codificación segura como la *Guía para proyectos abiertos de seguridad web* (consulte el Requisito 6.5 de las DSS de la PCI). ▪ Las correcciones pertinentes se implementan antes de su lanzamiento. ▪ La gerencia revisa y aprueba los resultados de la revisión de códigos antes de su lanzamiento.			
	6.3.7.c Seleccione la muestra de cambios recientes de aplicaciones personalizadas y controle que los códigos de aplicaciones personalizadas se revisen conforme a 6.3.7.a y 6.3.7.b que aparecen anteriormente.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.4 Siga los procedimientos de control de todos los cambios en los componentes del sistema. Los procedimientos deben incluir lo siguiente:	**6.4.a** Obtenga y evalúe los procedimientos de cambio de control de la empresa relacionados con la implementación de los parches de seguridad y las modificaciones de software y controle que los procedimientos incluyan los puntos 6.4.1 – 6.4.4 que aparecen a continuación.			
	6.4.b En el caso de la muestra de componentes de sistema y cambios o parches de seguridad recientes, realice un seguimiento de los cambios relacionados con la documentación de control de cambios. Por cada cambio que evalúe, realice lo siguiente:			
6.4.1 Documentación de incidencia	**6.4.1** Verifique que la documentación que tiene incidencia en el cliente se incluya en la documentación de control de cambios de cada cambio.			
6.4.2 Aprobación de la gerencia a cargo de las partes pertinentes	**6.4.2** Verifique que la aprobación de la gerencia a cargo de las partes pertinentes esté presente en cada cambio.			
6.4.3 Pruebas de la funcionalidad operativa	**6.4.3** Verifique que se realicen las pruebas de funcionalidad operativa para cada cambio.			
6.4.4 Procedimientos de desinstalación	**6.4.4** Verifique que se prepare los procedimientos de desinstalación para cada cambio			
6.5 Desarrolle todas las aplicaciones web (internas y externas, que incluyan el acceso administrativo web a la aplicación) basadas en las directrices de codificación segura, como la *Guía para proyectos de seguridad de aplicaciones web abiertas.* En los procesos de desarrollo de software, contemple la prevención de las vulnerabilidades comunes a la codificación, para incluir lo siguiente: *Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.10 estaban actualizadas en la guía OWASP cuando se publicó esta versión de las PCI DSS. Sin embargo, cuando la guía OWASP se actualice, debe usarse la versión vigente para estos requisitos.*	**6.5.a** Obtenga y revise los procesos de desarrollo de software de todas las aplicaciones basadas en la web. Verifique que los procesos exijan capacitación en técnicas de codificación segura para desarrolladores y que estén basados en guías como la guía OWASP (http://www.owasp.org).			
	6.5.b Entreviste a un grupo modelo de desarrolladores y obtenga pruebas de que son expertos en técnicas de codificación segura.			
	6.5.c Controle que existan procesos implementados para garantizar que las aplicaciones web no son vulnerables a lo siguiente:			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.5.1 Lenguaje de comandos entre distintos sitios (XSS)	**6.5.1** Lenguaje de comandos entre distintos sitios (XSS) (valide todos los parámetros antes de su inclusión).			
6.5.2 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección LDAP y Xpath, así como otros errores de inyección.	**6.5.2** Errores de inyección, en especial, errores de inyección SQL (valide la entrada para verificar que los datos del usuario no pueden modificar el significado de los comandos ni el de las consultas).			
6.5.3 Ejecución de archivos maliciosos	**6.5.3** Ejecución de archivos maliciosos (valide la entrada para verificar que la aplicación no acepte nombres de archivos ni archivos de los usuarios).			
6.5.4 Referencias inseguras a objetos directos	**6.5.4** Referencias inseguras a objetos directos (no exponga a los usuarios las referencias a objetos internos).			
6.5.5 Falsificación de solicitudes entre distintos sitios (CSRF)	**6.5.5** Falsificación de solicitudes entre distintos sitios (CSRF) (no confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente).			
6.5.6 Filtración de información y manejo inadecuado de errores	**6.5.6** Filtración de información y manejo inadecuado de errores (no filtre información por medio de mensajes de error u otros medios).			
6.5.7 Autenticación y administración de sesión interrumpidas	**6.5.7** Autenticación y administración de sesión interrumpidas (autentique correctamente a los usuarios y proteja las credenciales de cuentas y los tokens de sesión).			
6.5.8 Almacenamiento criptográfico inseguro	**6.5.8** Almacenamiento criptográfico inseguro (prevenga errores criptográficos).			
6.5.9 Comunicaciones inseguras	**6.5.9** Comunicaciones inseguras (cifre correctamente todas las comunicaciones autenticadas y confidenciales).			
6.5.10 Omisión de restringir el acceso URL	**6.5.10** Omisión de restringir el acceso a URL (refuerce constantemente el control del acceso en la capa de presentación y la lógica comercial para todas las URL).			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos de *alguno* de los siguientes métodos: ▪ Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio ▪ Instale un firewall de aplicación web enfrente de aplicaciones web públicas	**6.6** En el caso de aplicaciones web *públicas*, asegúrese de que se haya implementado *alguno* de los siguientes métodos: ▪ Controle que las aplicaciones web públicas se revisen (tanto mediante la utilización de herramientas o métodos manuales de evaluación de seguridad de vulnerabilidad como automáticos), de la siguiente manera: – Por lo menos, anualmente – Después de cualquier cambio – Por una organización que se especialice en seguridad de aplicaciones – Que se corrijan todas las vulnerabilidades – Que la aplicación se vuelva a analizar después de las correcciones ▪ Controle que se haya implementado un firewall de aplicación web delante de aplicaciones web públicas a los efectos de detectar y de evitar ataques basados en la web. *Nota: "La organización que se especializa en seguridad de aplicación" puede ser una tercera empresa o una organización interna, siempre que los revisores se especialicen en seguridad de aplicaciones y puedan demostrar independencia respecto del equipo de desarrollo.*			

Implemente medidas sólidas de control de acceso

Requisito 7: Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa

A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo.

"La necesidad de conocer" es la situación en que se otorgan derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso. Las limitaciones al acceso deben incluir lo siguiente:	**7.1** Obtenga y evalúe la política escrita sobre control de datos y controlar que la política incluya lo siguiente:			
7.1.1 Restricciones a los derechos de acceso a ID de usuarios privilegiadas a la menor cantidad de privilegios necesarios para cumplir con las responsabilidades del cargo	**7.1.1** Controle que los derechos de acceso a ID de usuarios privilegiadas se restrinjan a la menor cantidad de privilegios necesarios para cumplir con las responsabilidades del cargo.			
7.1.2 La asignación de privilegios se basa en la tarea del personal individual, su clasificación y función	**7.1.2** Controle que los privilegios se asignen a los individuos sobre la base de la clasificación y la función de su cargo (llamado "control de acceso basado en funciones" o RBAC).			
7.1.3 Los requisitos de un formulario de autorización escrito por la gerencia que detalle los privilegios solicitados	**7.1.3** Confirme que se necesite un formulario de autorización para todo acceso, que debe detallar los privilegios solicitados y que la gerencia debe firmar.			
7.1.4 Implementación de un sistema de control de acceso automático	**7.1.4** Controle que los controles de acceso se implementen a través de un sistema de control de acceso automático.			

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
7.2 Establezca un sistema de control de acceso para los componentes del sistema con usuarios múltiples que restrinja el acceso basado en la necesidad del usuario de conocer y se configure para "negar todos", salvo que se permita particularmente. Este sistema de control de acceso debe incluir lo siguiente:	**7.2** Evalúe los ajustes del sistema y la documentación del proveedor para controlar que un sistema de control de acceso se implemente de la siguiente manera:			
7.2.1 Cobertura de todos los componentes del sistema	**7.2.1** Controle que los sistemas de control de acceso se implementen en todos los componentes del sistema.			
7.2.2 La asignación de privilegios a individuos se basa en la clasificación del trabajo y la función	**7.2.2** Controle que los sistemas de control de acceso se configuren a los efectos de hacer cumplir los privilegios asignados a los individuos sobre la base de la clasificación de la tarea y la función.			
7.2.3 Ajuste predeterminado "negar todos"	**7.2.3** Controle que los sistemas de control de acceso posean un ajuste predeterminado de "negar todos". *Nota: Algunos sistemas de control de acceso se establecen de forma predeterminada para "permitir todos", y así permite acceso salvo que, o hasta que, se escriba una regla que niegue ese acceso en particular.*			

Requisito 8: Asigne una ID única a cada persona que tenga acceso a equipos.

La asignación de una identificación (ID) única a cada persona que tenga acceso garantiza que cada una de ellas es responsable de sus actos. Cuando se ejerce dicha responsabilidad, las acciones en datos críticos y sistemas las realizan usuarios conocidos y autorizados, y además se pueden realizar seguimientos.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.1 Asigne a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema y a datos de titulares de tarjetas.	**8.1** Verifique que todos los usuarios tengan asignada una ID única para tener acceso a componentes del sistema o titulares de tarjetas.			
8.2 Además de la asignación de una ID única**,** emplee al menos uno de los métodos siguientes para autenticar a los usuarios: ▪ Contraseña o frase de seguridad ▪ Autenticación de dos factores (por ejemplo, dispositivos token, tarjetas inteligentes, biometría o claves públicas)	**8.2** Para verificar que los usuarios se autentiquen con una ID única y una autenticación adicional (por ejemplo, una contraseña) para tener acceso al entorno de datos de titulares de tarjetas, realice lo siguiente: ▪ Obtenga y revise la documentación que describe los métodos de autenticación utilizados. ▪ Para cada tipo de método de autenticación utilizado y para cada tipo de componente del sistema, observe una autenticación para verificar que funcione de forma coherente con los métodos de autenticación documentado.			
8.3 Incorpore la autenticación de dos factores para el acceso remoto (acceso en el nivel de la red que se origina fuera de la red) a la red de empleados, administradores y terceros. Utilice tecnologías tales como autenticación remota y servicio dial-in (RADIUS); sistema de control de acceso mediante control del acceso desde terminales (TACACS) con tokens; o VPN (basada en SSL/TLS o IPSEC) con certificados individuales.	**8.3** Para verificar que se implemente la autenticación de dos factores para todos los accesos remotos a la red, observe a un empleado (por ejemplo a un administrador) al conectarse a la red de forma remota y verifique que se requieran tanto una clave como un elemento de autenticación adicional (por ejemplo, una tarjeta inteligente, token, PIN).			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.4 Deje ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una sólida criptografía (se define en *Glosario de términos, abreviaturas y acrónimos de las PCI DSS*).	**8.4.a** A modo de muestra de componentes del sistema, examine los archivos de las contraseñas para verificar que las contraseñas sean ilegibles durante la transmisión y el almacenamiento.			
	8.4.b Sólo para el caso de proveedores de servicio, observe los archivos de contraseñas para verificar que las contraseñas para clientes estén cifradas.			
8.5 Asegúrese de que sean correctas la autenticación del usuario y la administración de contraseñas de usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:	**8.5** Revise los procedimientos y entreviste al personal para verificar que se implementen los procedimientos de autenticación de usuarios y administración de contraseñas del siguiente modo:			
8.5.1 Controle el agregado, la eliminación y la modificación de las ID de usuario, las credenciales, entre otros objetos de identificación.	**8.5.1.a** Seleccione una muestra de ID de usuario, que incluya a administradores y usuarios generales. Verifique que cada usuario tenga autorización para utilizar el sistema de acuerdo con la política de la empresa mediante las siguientes acciones: ▪ Obtenga y examine un formulario de autorización de cada ID. ▪ Verifique que las ID de muestra se implementen de acuerdo con el formulario de autorización (que incluya privilegios especificados y todas las firmas obtenidas), mediante un seguimiento de la información del formulario de autorización al sistema.			
8.5.2 Verifique la identidad del usuario antes de restablecer contraseñas.	**8.5.2** Examine los procedimientos de contraseña y observe al personal de seguridad para verificar que, si un usuario solicita restablecer una contraseña vía telefónica, correo electrónico, Internet u otro método no personal, la identidad de dicho usuario se verifique antes del restablecimiento de la contraseña.			
8.5.3 Configure la primera contraseña en un valor único para cada usuario y cámbiela de inmediato después del primer uso.	**8.5.3** Examine los procedimientos de contraseña y observe al personal de seguridad para verificar que las primeras contraseñas para nuevos usuarios se configuren en un valor único para cada usuario y se cambien después del primer uso.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.4 Cancele de inmediato el acceso para cualquier usuario cesante.	**8.5.4** Seleccione una muestra de empleados cesantes en los últimos seis meses y revise las listas de acceso de usuario actuales para verificar que sus ID se hayan desactivado o eliminado.			
8.5.5 Elimine/desactive las cuentas de usuario al menos cada 90 días.	**8.5.5** Verifique que se eliminen o se desactiven las cuentas que lleven más de 90 días inactivas.			
8.5.6 Active las cuentas que utilicen los proveedores para el mantenimiento remoto únicamente durante el período necesario.	**8.5.6** Verifique que cualquiera de las cuentas que utilicen los proveedores para soporte y mantenimiento de los componentes del sistema estén desactivadas, que el proveedor las active sólo cuando sea necesario y que sean controladas durante su uso.			
8.5.7 Informe los procedimientos y políticas de contraseñas a todos los usuarios que tengan acceso a datos de titulares de tarjetas.	**8.5.7** Entreviste a los usuarios de una muestra de ID de usuario para verificar que estén familiarizados con los procedimientos y políticas de contraseñas.			
8.5.8 No utilice cuentas ni contraseñas grupales, compartidas o genéricas.	**8.5.8.a** A modo de prueba de componentes del sistema, examine las listas de ID de usuario y verifique lo siguiente ▪ Las ID de usuario y cuentas genéricas se encuentran desactivadas o se han eliminado. ▪ No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. ▪ Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.			
	8.5.8.b Examine las políticas/procedimientos de contraseñas para comprobar que las contraseñas de grupo y compartidas estén prohibidas de manera explícita.			
	8.5.8.c Entreviste a los administradores del sistema para verificar que las contraseñas de grupo y compartidas no se distribuyan, aunque sean solicitadas.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.9 Cambie las contraseñas de usuario al menos cada 90 días.	**8.5.9** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se solicite al usuario cambiar su contraseña al menos cada 90 días. Para proveedores de servicio únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite periódicamente que el cliente cambie la contraseña y que éste reciba ayuda para saber cuándo y bajo qué circunstancias debe cambiarla.			
8.5.10 Solicite una longitud de contraseña mínima de siete caracteres.	**8.5.10** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se solicite que la contraseña tenga al menos siete caracteres. Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de cliente cumplan con un requisito mínimo de cantidad de caracteres.			
8.5.11 Utilice contraseñas que contengan tanto caracteres numéricos como alfabéticos.	**8.5.11** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se solicite que incluyan caracteres numéricos y alfabéticos. Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de cliente incluyan tanto caracteres numéricos como alfabéticos.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.12 No permita que ninguna persona envíe una contraseña nueva igual a cualquiera de las últimas cuatro contraseñas utilizadas.	**8.5.12** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se solicite que las nuevas contraseñas no sean iguales a las últimas cuatro contraseñas utilizadas anteriormente. Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que las nuevas contraseñas de cliente no puedan ser iguales que las cuatro contraseñas utilizadas anteriormente.			
8.5.13 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.	**8.5.13** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se solicite que se bloquee la cuenta del usuario después de no más de seis intentos de inicio de sesión no válidos. Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que las cuentas cliente se bloqueen de forma temporal después de no más de seis intentos no válidos de acceso.			
8.5.14 Establezca la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.	**8.5.14** A modo de muestra de componentes del sistema, sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que se solicite que una vez que se bloquea la cuenta de un usuario, ésta permanezca bloqueada durante un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.			
8.5.15 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para que se active la terminal nuevamente.	**8.5.15** A modo de muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que las funciones de tiempo máximo de inactividad del sistema/sesión se encuentren establecidos en 15 minutos o menos.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.16 Autentique todos los accesos a cualquier base de datos que contenga datos de titulares de tarjetas. Esto incluye el acceso de aplicaciones, administradores y demás usuarios.	**8.5.16.a** Revise los parámetros de configuración de base de datos y aplicaciones, y verifique que la autenticación del usuario y el acceso a la base de datos incluyan lo siguiente: ▪ Todos los usuarios sean autenticados antes de obtener acceso. ▪ Todo acceso de usuario, consultas de usuario y acciones de usuario (por ejemplo, mover, copiar, eliminar) en la base se datos se realicen únicamente mediante métodos programáticos (por ejemplo, a través de procedimientos almacenados). ▪ El acceso directo a o las consultas en las bases de datos se restrinjan a los administradores de la base de datos.			
	8.5.16.b Revise las aplicaciones de la base de datos y las ID de aplicaciones relacionadas para verificar que las ID de aplicación las puedan utilizar sólo las aplicaciones (y no los usuarios u otros procesos).			

Requisito 9: Restrinja el acceso físico a datos de titulares de tarjetas.

Cualquier acceso físico a datos o sistemas que alojen datos de titulares de tarjetas permite el acceso a dispositivos y datos, así como también permite la eliminación de sistemas o copias en papel, y se debe restringir correctamente.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.1 Utilice controles de entrada a la empresa para limitar y supervisar el acceso a sistemas en el entorno de datos de titulares de tarjetas.	**9.1** Verifique la existencia de controles de seguridad física para cada sala de informática, centro de datos y otras áreas físicas con sistemas en el entorno de datos de titulares de tarjetas. ▪ Verifique que se controle el acceso con lectores de placas de identificación u otros dispositivos, incluidas placas autorizadas y llave y candado. ▪ Observe un intento de algún administrador del sistema para iniciar sesión en las consolas de sistemas seleccionados de forma aleatoria en un entorno de titulares de tarjetas y verifique que estén "aseguradas" y se impida el uso no autorizado.			
9.1.1 Utilice cámaras de video u otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario. *Nota: "Áreas confidenciales" hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. No se incluyen las áreas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.*	**9.1.1** Verifique que las cámaras de video u otros mecanismos de control de acceso estén funcionando correctamente para supervisar los puntos de entrada/salida de áreas confidenciales. Las cámaras de video u otros mecanismos deben contar con protección contra alteraciones y desactivaciones. Verifique que las cámaras de video u otros mecanismos se supervisen y los datos de dichas cámaras o mecanismos se almacenen durante al menos tres meses.			
9.1.2 Restrinja el acceso físico a conexiones de red de acceso público.	**9.1.2** Verifique que sólo empleados autorizados activen las conexiones de red sólo cuando sea necesario realizando entrevistas y observando. Por ejemplo, las salas de conferencias utilizadas para alojar visitantes no deben tener puertos de red activados con DHCP. De forma alternativa, verifique que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.1.3 Restrinja el acceso físico a puntos de acceso inalámbrico, puertas de enlace y dispositivos manuales.	**9.1.3** Restrinja el acceso físico a puntos de acceso inalámbrico, puertas de enlace y dispositivos manuales se encuentre restringido adecuadamente.			
9.2 Desarrolle procedimientos para que el personal pueda distinguir con facilidad entre empleados y visitantes, especialmente en las áreas donde se puede acceder fácilmente a datos de titulares de tarjetas. *A los fines de este requisito, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la entidad. "Visitante" se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones de la empresa durante un tiempo no prolongado, generalmente no más de un día.*	**9.2.a** Revise los procesos y procedimientos para la asignación de placas de identificación a los empleados, y a visitantes, y verifique que estos procesos incluyan lo siguiente: ▪ Otorgamiento de nuevas placas de identificación, cambio de requisitos de acceso y anulación de empleados cesantes y placas vencidas de visitantes ▪ Sistema limitado de placas de identificación de acceso			
	9.2.b Observe a las personas que se encuentren en las instalaciones de la empresa y verifique que resulte sencillo distinguir entre empleados y visitantes.			
9.3 Asegúrese de que todos los visitantes reciban el siguiente trato:	**9.3** Verifique que los controles realizados a empleados/visitantes se implementen de la siguiente manera:			
9.3.1 Autorización previa al ingreso a áreas en las que se procesan o se conservan datos de titulares de tarjetas	**9.3.1** Observación de visitantes para verificar que se utilicen las placas de identificación para visitantes. Intente obtener acceso al centro de datos para verificar que ninguna placa de identificación para visitantes permita el acceso sin acompañante a áreas físicas donde se almacenen datos de titulares de tarjetas.			
9.3.2 Token físico otorgado (por ejemplo una placa de identificación o dispositivo de acceso) con vencimiento y que identifique a los visitantes como personas no pertenecientes a la empresa	**9.3.2** Examine las placas de identificación para empleados y visitantes para verificar que dichas placas diferencien con claridad a los empleados de los visitantes/personas ajenas y que la placa tenga vencimiento.			
9.3.3 Solicitud de entrega del token físico antes de salir de las instalaciones de la empresa o al momento del vencimiento	**9.3.3** Observe la salida de los visitantes de las instalaciones de la empresa para verificar que se solicite la entrega de sus placas de identificación al partir, o al momento del vencimiento.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.4 Use un registro de visitas para implementar una pista de auditoría física de la actividad de visitas. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.	**9.4.a** Verifique que haya un registro de visitas en uso para registrar el acceso físico a las instalaciones de la empresa, así como también a las salas de informática y los centros de datos donde se guardan o se transmiten los datos de titulares de tarjetas.			
	9.4.b Verifique que el registro incluya el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico y consérvelo durante tres meses como mínimo.			
9.5 Almacene los medios de copias de seguridad en un lugar seguro, preferentemente en un lugar externo a la empresa, como un centro alternativo o para copias de seguridad, o un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.	**9.5** Verifique que el lugar de almacenamiento se revise una vez al año al menos para determinar que el almacenamiento de medios de copia de seguridad sea seguro.			
9.6 Resguarde de forma física todos los papeles y dispositivos electrónicos que contengan datos de titulares de tarjetas.	**9.6** Verifique que los procedimientos para proteger los datos de titulares de tarjetas incluyan controles para el resguardo seguro de papel y dispositivos electrónicos (incluidas computadoras, dispositivos electrónicos extraíbles, redes y hardware de comunicación, líneas de telecomunicación, recibos en papel, informes en papel y faxes).			
9.7 Lleve un control estricto sobre la distribución interna o externa de cualquier tipo de medios que contenga datos de titulares de tarjetas, incluidos:	**9.7** Verifique que exista una política para controlar la distribución de medios que contengan datos de titulares de tarjetas y que dicha política abarque todos los medios distribuidos, incluso los que se distribuyen a personas.			
9.7.1 Clasifique los medios de manera que se puedan identificar como confidenciales.	**9.7.1** Verifique que todos los medios estén clasificados de manera que se puedan identificar como “confidenciales”.			
9.7.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.	**9.7.2** Verifique que todos los medios enviados fuera de la empresa esté registrado y cuente con la autorización de la gerencia, así como también que se envíe por correo seguro u otro método de envío que se pueda rastrear.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura (especialmente cuando se los distribuye a personas).	**9.8** Seleccione una muestra actual de varios días de registros de seguimiento externos de todos los medios que contengan datos de titulares de tarjetas y verifique la presencia en los registros de detalles de seguimiento y la debida autorización de la gerencia.			
9.9 Lleve un control estricto sobre el almacenamiento y accesibilidad de los medios que contengan datos de titulares de tarjetas.	**9.9** Obtenga y examine la política para controlar el almacenamiento y mantenimiento de copias en papel y dispositivos electrónicos, y verifique que la política requiera inventarios periódicos de medios.			
9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	**9.9.1** Obtenga y revise el registro de inventario de medios para verificar que se realicen inventarios periódicos de medios al menos una vez al año.			
9.10 Destruya los medios que contengan datos de titulares de tarjetas cuando ya no sea necesario para la empresa o por motivos legales, de la siguiente manera:	**9.10** Obtenga y examine periódicamente la política de destrucción de medios y verifique que abarque todos los medios que contengan datos de titulares de tarjetas y confirme lo siguiente:			
9.10.1 Corte en tiras, incinere o haga pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas.	**9.10.1.a** Verifique que los materiales de copias en papel se corten de manera cruzada, se incineren o se hagan pasta de manera tal que se tenga la seguridad de que no podrán reconstruirse los materiales de la copia en papel.			
	9.10.1.b Examine los contenedores de almacenamiento utilizados para la destrucción de información para verificar que dichos recipientes estén asegurados. Por ejemplo, verifique que el recipiente para corte en tiras cuente con una traba para impedir el acceso a su contenido.			
9.10.2 Entregue los datos de titulares de tarjetas en dispositivos electrónicos no recuperables para que dichos datos no se puedan reconstruir.	**9.10.2** Verifique que los datos de titulares de tarjetas guardados en dispositivos electrónicos sean irrecuperables y se entreguen mediante un programa con la función de borrado seguro de acuerdo con las normas aceptadas en la industria para lograr una eliminación segura, o bien destruya los medios de forma física (por ejemplo, degaussing o destrucción magnética).			

Supervise y pruebe las redes con regularidad

Requisito 10: Rastree y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.

Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el rastreo, alertas y análisis cuando algo no funciona bien. La determinación de la causa de algún riesgo es muy difícil sin los registros de la actividad del sistema.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
10.1 Establezca un proceso para vincular todos los accesos a componentes del sistema (especialmente el acceso con privilegios administrativos, tales como de raíz) a cada usuario en particular.	**10.1** Mediante observación y entrevistas al administrador del sistema, verifique que las pistas de auditoría estén habilitadas y activas para los componentes del sistema.			
10.2 Implemente pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos:	**10.2** Mediante entrevistas, exámenes de los registros de auditoría y exámenes de los parámetros de los registros de auditoría, realice lo siguiente:			
10.2.1 Todo acceso de personas a datos de titulares de tarjetas	**10.2.1** Verifique que esté registrado todo acceso de personas a datos de titulares de tarjetas.			
10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos	**10.2.2** Verifique que estén registradas todas las acciones realizadas por personas con privilegios de raíz o administrativos			
10.2.3 Acceso a todas las pistas de auditoría	**10.2.3** Verifique que esté registrado el acceso a todas las pistas de auditoría			
10.2.4 Intentos de acceso lógico no válidos	**10.2.4** Verifique que estén registrados todos los intentos de acceso lógico no válidos			
10.2 5 Uso de mecanismos de identificación y autenticación	**10.2.5** Verifique que esté registrado el uso de mecanismos de identificación y autenticación.			
10.2.6 Inicialización de los registros de auditoría	**10.2.6** Verifique que esté registrada la inicialización de los registros de auditoría.			
10.2.7 Creación y eliminación de objetos en el nivel del sistema.	**10.2.7** Verifique que estén registrados la creación y la eliminación de objetos en el nivel del sistema.			
10.3 Registre al menos las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:	**10.3** Mediante entrevistas y observación, realice lo siguiente para cada evento auditable (de 10.2):			
10.3.1 Identificación de usuarios	**10.3.1** Verifique que la identificación de usuarios se encuentre incluida en las entradas del registro.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
10.3.2 Tipo de evento	**10.3.2** Verifique que el tipo de evento se incluya en las entradas del registro.			
10.3.3 Fecha y hora	**10.3.2** Verifique que el sello de fecha y hora se incluya en las entradas del registro.			
10.3.4 Indicación de éxito u omisión	**10.3.2** Verifique que la indicación de éxito u omisión se incluya en las entradas del registro.			
10.3.2 Origen del evento	**10.3.2** Verifique que el origen del evento se incluya en las entradas del registro.			
10.3.6 Identidad o nombre de los datos, componentes del sistema o recurso afectados	**10.3.6** Verifique que la identidad o nombre de los datos, componentes del sistema o recursos afectados estén incluidos en las entradas del registro.			
10.4 Sincronice todos los relojes y horarios críticos del sistema.	**10.4** Obtenga y revise el proceso de adquisición y distribución del horario correcto en la organización, así como también los parámetros del sistema relacionados con la hora a modo de muestra de componentes del sistema. Verifique que se incluya y se implemente lo siguiente en el proceso:			
	10.4.a Verifique que se utilice una versión estable y conocida de servidores NTP (Network Time Protocol) o tecnología similar, actualizados según los requisitos 6.1 y 6.2 de las PCI DSS para la sincronización de hora.			
	10.4.b Verifique que los servidores internos no estén recibiendo señales de hora de orígenes externos. [Dos o tres servidores centrales de hora de la organización reciben señales de hora externas [directamente de una radio especial, satélites GPS u otros orígenes externos basados en el tiempo atómico internacional (TAI) y UTC (anteriormente GMT)], emparéjelos para mantener la hora exacta y distribuya la hora a otros servidores internos].			
	10.4.c Verifique que se designen host externos específicos desde los cuales los servidores de hora aceptarán las actualizaciones de horario de NTP (para evitar que cualquier persona malintencionada cambie el reloj). De forma opcional, se pueden cifrar estas actualizaciones con una clave simétrica, y se pueden crear listas de control de acceso que especifiquen las direcciones IP de equipos cliente que se proporcionarán con el servicio NTP (para evitar el uso no autorizado de servidores de hora internos). Consulte www.ntp.org para obtener más información			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.	**10.5** Entreviste al administrador del sistema y examine los permisos para verificar que las pistas de auditoría sean seguras y que no se puedan modificar de la siguiente manera:			
10.5.1 Limite la visualización de pistas de auditoría a quienes lo necesiten por motivos de trabajo.	**10.5.1** Verifique que sólo las personas que lo necesiten por motivos relacionados con el trabajo puedan visualizar los archivos de las pistas de auditoría.			
10.5.2 Proteja los archivos de las pistas de auditoría contra las modificaciones no autorizadas.	**10.5.2** Verifique que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes.			
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de inmediato en un servidor de registros central o medios que resulten difíciles de modificar.	**10.5.3** Verifique que se haya realizado copia de seguridad de los archivos actuales de las pistas de auditoría inmediatamente en un servidor de registros central o medios que resulten difíciles de modificar.			
10.5.4 Escriba registros para tecnologías externas en un servidor de registros en la LAN interna.	**10.5.4** Verifique que los registros para tecnologías externas (por ejemplo, inalámbricas, firewalls, DNS, correo) se descarguen o se copien en un servidor de registros central o medios internos.			
10.5.5 Utilice el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).	**10.5.5** Verifique el uso del software de monitorización de integridad de archivos o de detección de cambios para registros mediante el análisis de los parámetros del sistema, de los archivos monitorizados y de los resultados de dicha monitorización.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
10.6 Revise los registros de todos los componentes del sistema al menos una vez al día. Las revisiones de registros incluyen a los servidores que realizan funciones de seguridad, tales como sistema de detección de intrusiones (IDS) y servidores de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS). *Nota: las herramientas de recolección, análisis y alerta de registros pueden ser utilizadas para cumplir con el requisito 10.6*	**10.6.a** Obtenga y examine las políticas y procedimientos de seguridad para verificar la inclusión de procedimientos de revisión de registros de seguridad al menos una vez al día y que se requiera el seguimiento de las excepciones.			
	10.6.b Mediante observación y entrevistas, verifique que se realicen revisiones de registros regularmente de todos los componentes del sistema.			
10.7 Conserve el historial de pista de auditorías durante al menos un año, con un mínimo de tres meses inmediatamente disponible para el análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).	**10.7.a** Obtenga y examine las políticas y procedimientos de seguridad y verifique que se incluyan las políticas de retención de registros de auditoría y que se requiera la conservación del registro de auditoría durante al menos un año.			
	10.7.b Verifique que los registros de auditoría se encuentren disponibles durante al menos un año y que se implementen los procesos para restaurar al menos los registros de los últimos tres meses para el análisis inmediato.			

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.

Las vulnerabilidades ocasionadas por personas malintencionadas e investigadores se descubren continuamente, y se introducen mediante software nuevo. Los componentes, procesos y software personalizado del sistema se deben probar con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.1 Las pruebas para comprobar la presencia de puntos de acceso inalámbricos mediante el uso de un analizador inalámbrico al menos trimestralmente o la implementación de un sistema de detección de intrusiones (IDS)/sistema contra intrusos (IPS) inalámbrico para identificar todos los dispositivos inalámbricos en uso.	**11.1.a** Verifique que el analizador inalámbrico se utilice al menos trimestralmente o que se implemente el IDS/IPS inalámbrico, configurado para identificar todos los dispositivos inalámbricos.			
	11.1.b Si se implementa un IDS/IPS inalámbrico, verifique que la configuración genere alertas al personal.			
	11.1 c Verifique que el Plan de respuesta a incidentes de la organización (Requisito 12.9) incluya una respuesta en caso de que se detecten dispositivos inalámbricos no autorizados.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.2 Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos). *Nota: los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor Aprobado de Escaneo (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). Los análisis realizados después de cambios en la red puede realizarlos el personal interno de la empresa.*	**11.2.a** Inspeccione los resultados de los últimos cuatro trimestres de los análisis de la red interna, host y vulnerabilidad de aplicaciones para verificar que se realicen las pruebas de seguridad periódicas de los dispositivos dentro del entorno de datos de los titulares de tarjetas. Verifique que el proceso de análisis incluya nuevos análisis hasta que se obtengan resultados aprobados. *Nota: los análisis externos que se realizan después de cambios en la red y análisis internos pueden realizarlos tanto personal capacitado de la empresa como personas externas.*			
	11.2.b Verifique que se estén realizando análisis trimestralmente de acuerdo con los procedimientos de análisis de seguridad de PCI, mediante la inspección de los resultados de los últimos cuatro trimestres de análisis de vulnerabilidades externas y verifique que: ▪ se hayan realizado cuatro análisis trimestrales en el último período de 12 meses; ▪ los resultados de cada análisis cumplan con los procedimientos de análisis de seguridad de PCI (por ejemplo, que no existan vulnerabilidades urgentes, críticas ni elevadas); ▪ los análisis los haya completado un Proveedor Aprobado de Escaneo (ASV) certificado por PCI SSC. *Nota: no se requiere que se completen cuatro análisis trimestrales aprobados para el cumplimiento inicial de PCI DSS si el asesor verifica que 1) el resultado del último análisis fue un análisis aprobado, 2) la entidad ha documentado políticas y procedimientos que exigen análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. Durante los años posteriores a la revisión inicial de PCI DSS, se deben haber realizado análisis trimestrales aprobados.*			
	11.2.c Verifique que se realicen análisis internos y/o externos después de cualquier cambio significativo en la red, mediante la inspección de los resultados de los análisis del último año. Verifique que el proceso de análisis incluya nuevos análisis hasta que se obtengan resultados aprobados.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.3 Realice pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno). Estas pruebas de penetración deben incluir lo siguiente:	**11.3.a** Obtenga y examine los resultados de la última prueba de penetración para verificar que dichas pruebas se realicen al menos anualmente y después de cualquier cambio significativo realizado en el entorno. Verifique que las vulnerabilidades detectadas se hayan corregido y que se repitan las pruebas.			
	11.3.b Verifique que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado, y cuando corresponda, que la persona que realice la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).			
11.3.1 Pruebas de penetración de la capa de red	**11.3.1** Verifique que la prueba de penetración incluya pruebas de penetración de la capa de red. Dichas pruebas deben incluir a los componentes que admiten las funciones de red, así como también a los sistemas operativos.			
11.3.2 Pruebas de penetración de la capa de aplicación	**11.3.2** Verifique que la prueba de penetración incluya pruebas de penetración de la capa de aplicación. En el caso de aplicaciones Web, las pruebas deben incluir, como mínimo, las vulnerabilidades enumeradas en el Requisito 6.5.			
11.4 Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de detección y prevención de intrusiones.	**11.4.a** Verifique el uso de sistemas de detección y/o prevención de intrusiones, y que se supervise el tráfico en el entorno de titulares de tarjetas.			
	11.4.b Confirme que estén configurados el IDS y/o IPS para alertar al personal ante la sospecha de riesgos.			
	11.4.c Examine la configuración de IDS/IPS y confirme que los dispositivos de IDS/IPS estén configurados, se mantengan y se actualicen según las instrucciones del proveedor para garantizar una protección óptima.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.5 Implemente el software de monitorización de integridad de archivos para alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de configuración o archivos de contenido; asimismo configure el software para realizar comparaciones de archivos críticos al menos semanalmente. *Nota: a los fines de la monitorización de integridad de archivos, los archivos críticos generalmente son los que no se modifican con regularidad, pero cuya modificación podría indicar un riesgo o peligro para el sistema. Los productos para la monitorización de integridad de archivos generalmente vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.*	**11.5** Verifique el uso de los productos para monitorización de integridad de archivos en el entorno de datos de titulares de tarjetas mediante la observación de la configuración del sistema y los archivos monitorizados, así como también de la revisión de los resultados de las actividades de monitorización. Ejemplos de archivos que se deben monitorizar: ▪ Ejecutables del sistema ▪ Ejecutables de aplicaciones ▪ Archivos de configuración y parámetros ▪ Archivos de almacenamiento central, históricos o archivados, de registro y auditoría			

Mantenga una política de seguridad de la información

Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.

Una política de seguridad sólida establece el grado de seguridad para toda la empresa e informa a los empleados lo que se espera de ellos. Todos los empleados deben estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos. A los fines de este requisito, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la empresa.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.1 Establezca, publique, mantenga y distribuya una política de seguridad que logre lo siguiente:	**12.1** Examine la política de seguridad de la información y verifique que la política se publique y se distribuya a los usuarios del sistema que corresponda (incluidos proveedores, contratistas y socios comerciales).			
12.1.1 Aborde todos los requisitos de PCI DSS.	**12.1.1** Verifique que la política aborde todos los requisitos de PCI DSS.			
12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	**12.1.2** Verifique que la política de seguridad de la información incluya un proceso de evaluación formal de riesgos que identifique las amenazas, las vulnerabilidades y los resultados de una evaluación formal de riesgos.			
12.1.3 Incluya una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	**12.1.3** Verifique que la política de seguridad de la información se revise al menos una vez al año y se actualice según sea necesario de manera que refleje los cambios en los objetivos de la empresa o el entorno de riesgos.			
12.2 Desarrolle procedimientos diarios de seguridad operativa coherentes con los requisitos de esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas de usuarios y procedimientos de revisión de registros).	**12.2.a** Examine los procedimientos diarios de seguridad operativa. Verifique que coincidan con esta especificación e incluyan procedimientos administrativos y técnicos para cada uno de los requisitos.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.3 Desarrolle políticas de utilización para tecnologías críticas para empleados (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, asistentes digitales/para datos personales [PDA], utilización del correo electrónico Internet) para definir el uso adecuado de dichas tecnologías por parte de empleados y contratistas. Asegúrese de que estas políticas de uso requieran lo siguiente:	**12.3** Obtenga y examine la política de tecnologías críticas para empleados y realice lo siguiente:			
12.3.1 Aprobación explícita de la gerencia	**12.3.1** Verifique que las políticas de uso requieran aprobación explícita de la gerencia para utilizar las tecnologías.			
12.3.2 Autenticación para el uso de la tecnología	**12.3.2** Verifique que las políticas de uso requieran que todo uso de tecnologías se autentique con ID de usuario y contraseña, u otro elemento de autenticación (por ejemplo, token).			
12.3.3 Lista de todos los dispositivos y personal que tenga acceso	**12.3.3** Verifique que las políticas de uso requieran una lista de todos los dispositivos y personal autorizado para utilizar los dispositivos.			
12.3.4 Etiquetado de dispositivos con propietario, información de contacto y objetivo	**12.3.4** Verifique que las políticas de uso requieran etiquetado de los dispositivos con propietario, información de contacto y objetivo			
12.3.5 Usos aceptables de la tecnología	**12.3.5** Verifique que las políticas de uso requieran usos aceptables de la tecnología.			
12.3.6 Ubicaciones aceptables de las tecnologías en la red	**12.3.6** Verifique que las políticas de uso requieran ubicaciones aceptables de la tecnología en la red.			
12.3.7 Lista de productos aprobados por la empresa	**12.3.7** Verifique que las políticas de uso requieran una lista de productos aprobados por la empresa.			
12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad	**12.3.8** Verifique que las políticas de uso requieran la desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.3.9 Activación de tecnologías de acceso remoto para proveedores sólo cuando estos lo requieren, con desactivación automática después de la utilización	**12.3.9** Verifique que las políticas de uso requieran la activación de tecnologías de acceso remoto para proveedores sólo cuando estos lo requieren, con desactivación automática después de la utilización.			
12.3.10 Al tener acceso a datos de titulares de tarjetas mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles.	**12.3.10** Verifique que las políticas de uso prohíban copiar, mover o almacenar datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto.			
12.4 Asegúrese de que las políticas y procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todos los empleados y contratistas.	**12.4** Verifique que las políticas de seguridad de la información definan con claridad las responsabilidades de seguridad de la información tanto para empleados como para contratistas.			
12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo:	**12.5** Verifique que se asigne formalmente la seguridad de la información a un Jefe de seguridad u otro miembro de la gerencia relacionado con la seguridad. Obtenga y examine las políticas y procedimientos de seguridad de la información para verificar que se asignen específicamente las siguientes responsabilidades de seguridad de la información:			
12.5.1 Establezca, documente y distribuya políticas y procedimientos de seguridad.	**12.5.1** Verifique que la responsabilidad de crear y distribuir políticas y procedimientos de seguridad haya sido formalmente asignada.			
12.5.2 Supervise y analice las alertas e información de seguridad, y distribúyalas entre el personal correspondiente.	**12.5.2** Verifique que se haya asignado formalmente la responsabilidad de la supervisión y análisis de alertas de seguridad y la distribución de información al personal correspondiente a las unidades de seguridad de la información y comercial.			
12.5.3 Establezca, documente y distribuya los procedimientos de respuesta ante incidentes de seguridad y escalación para garantizar un manejo oportuno y efectivo de todas las situaciones.	**12.5.1** Verifique que la responsabilidad de crear y distribuir procedimientos de respuesta ante incidentes de seguridad y escalación haya sido formalmente asignada.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.5.4 Administre las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones	**12.5.4** Verifique que la responsabilidad de administración de cuentas y gestión de autenticación se haya asignado formalmente.			
12.5.5 Supervise y controle todo acceso a datos.	**12.5.5** Verifique que la responsabilidad de supervisar y controlar todo acceso a datos se haya asignado formalmente.			
12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	**12.6.a** Verifique la existencia de un programa formal de concienciación sobre seguridad para todos los empleados.			
	12.6.b Obtenga y examine los procedimientos y la documentación del programa de concienciación sobre seguridad y realice lo siguiente:			
12.6.1 Eduque a los empleados al contratarlos y al menos una vez al año.	**12.6.1.a** Verifique que el programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los empleados en lo relativo a la concienciación (por ejemplo, carteles, cartas, notas, capacitación basada en Web, reuniones y promociones).			
	12.6.1.b Verifique que los empleados concurran a la capacitación sobre concienciación al ser contratados y al menos una vez al año.			
12.6.2 Exija a los empleados que reconozcan al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa.	**12.6.2** Verifique que el programa de concienciación sobre seguridad exija a los empleados que reconozcan (por ejemplo, por escrito o de forma electrónica) al menos una vez al año haber leído y entendido la política de seguridad de la información de la empresa.			
12.7 Examine a los posibles empleados (consulte la definición de "empleado" en 9.2 más arriba) antes de contratarlos a los fines de minimizar el riesgo de ataques provenientes de orígenes internos. *En el caso de empleados tales como cajeros de un comercio, que sólo tienen acceso a un número de tarjeta a la vez al realizarse una transacción, este requisito constituye sólo una recomendación.*	**12.7** Consulte con la gerencia del departamento de Recursos Humanos y compruebe que se realicen las verificaciones de antecedentes de los empleados (dentro de los límites de las leyes locales) antes de la contratación de quien tendrá acceso a datos de titulares de tarjetas o al entorno de los datos de titulares de tarjetas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias).			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.8 Si los datos de titulares de tarjeta se comparten con proveedores de servicios, mantenga e implemente políticas y procedimientos a los fines de que los proveedores de servicio incluyan lo siguiente:	**12.8** Si la entidad que se evalúa comparte datos de titulares de tarjetas con proveedores de servicios (por ejemplo, centros de almacenamiento de copias de seguridad en cinta, proveedores de servicios gestionados tales como empresas de Web hosting o proveedores de servicios de seguridad, o bien quienes reciben datos para el diseño de modelos de fraude), mediante la observación, la revisión de políticas y procedimientos y de la documentación de respaldo, realice lo siguiente:			
12.8.1 Mantenga una lista de proveedores de servicios.	**12.8.1** Verifique que se mantenga una lista de proveedores de servicios.			
12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	**12.8.2** Verifique que el acuerdo escrito incluya una mención del proveedor de servicios respecto de su responsabilidad por la seguridad de los datos de titulares de tarjetas.			
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	**12.8.3** Verifique que las políticas y procedimientos se encuentren documentadas y que se haya realizado un seguimiento que incluya una auditoría adecuada previa al compromiso con cualquier proveedor de servicios.			
12.8.4 Mantenga un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios.	**12.8.4** Verifique que la entidad evaluada mantenga un programa para supervisar el estado de cumplimiento con PCI DSS del proveedor de servicios.			
12.9 Implemente un plan de respuesta a incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.	**12.9** Obtenga y examine el plan de respuesta a incidentes y los procedimientos relacionados y realice lo siguiente:			

(12.9 continúa en la página siguiente)

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.9.1 Cree el plan de respuesta a incidentes que se va a implementar en caso de fallos en el sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: ▪ Funciones, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. ▪ Procedimientos específicos de respuesta a incidentes. ▪ Procedimientos de recuperación y continuidad comercial. ▪ Procesos de realización de copia de seguridad de datos. ▪ Análisis de los requisitos legales para el informe de riesgos. ▪ Cobertura y respuestas de todos los componentes críticos del sistema. ▪ Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.	**12.9.1** Verifique que el plan de respuesta a incidentes incluya: ▪ funciones, responsabilidades y estrategias de comunicación en caso de un riesgo que incluya como mínimo la notificación de las marcas de pago; ▪ procedimientos específicos de respuesta a incidentes; ▪ procedimientos de recuperación y continuidad comercial; ▪ procesos de realización de copia de seguridad de datos; ▪ análisis de requisitos legales para el informe de riesgos (por ejemplo, la ley 1386 del Senado de California que exige la notificación de los consumidores afectados en caso de un riesgo real o sospechado por operaciones comerciales con residentes de California en su base de datos); ▪ cobertura y respuestas de todos los componentes críticos del sistema; ▪ referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.			
12.9.2 Pruebe el plan al menos una vez al año.	**12.9.2** Verifique que se realice una prueba del plan al menos una vez al año.			
12.9.3 Designe personal especializado que se encuentre disponible permanentemente para responder a las alertas.	**12.9.3** Mediante la observación y revisión de las políticas, verifique que haya respuesta permanente a incidentes y cobertura de monitorización para cualquier evidencia de actividad no autorizada, detección de puntos de acceso inalámbricos no autorizados, alertas críticas de IDS y/o informes de cambios no autorizados en archivos críticos o de contenido.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.9.4 Proporcione capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad.	**12.9.4** Mediante la observación y revisión de las políticas, verifique que se capacite periódicamente al personal en cuanto a las responsabilidades de fallos de seguridad.			
12.9.5 Incluya alertas de sistemas de detección y prevención de intrusiones, y de monitorización de integridad de archivos.	**12.9.5** Mediante observación y revisión de los procesos, verifique que el plan de respuestas a incidentes abarque la monitorización y la respuesta a alertas de los sistemas de seguridad, así como también la detección de puntos de acceso inalámbricos no autorizados.			
12.9.6 Elabore un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria.	**12.9.6** Mediante observación y revisión de políticas, verifique que exista un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria.			

Anexo A: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido

Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas

Tal como se menciona en el Requisito 12.8, todos los proveedores de servicios con acceso a datos de titulares de tarjetas (incluidos los proveedores de hosting compartido) deben adherirse a PCI DSS. Además, el requisito 2.4 establece que los proveedores de hosting compartido deben proteger el entorno y los datos que aloja cada entidad. Por lo tanto, los proveedores de hosting compartido deben cumplir además con los requisitos de este Anexo.

Requisitos	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicio u otra entidad), según A.1.1 a A.1.4: Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS. *Nota: aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad* debe *cumplir con las PCI DSS y validar el cumplimiento según corresponda.*	**A.1** Específicamente en el caso de la evaluación de PCI DSS de un proveedor de hosting compartido en la que se verifique que los proveedores de hosting compartido protegen el entorno y los datos que alojan las entidades (comerciantes y proveedores de servicios), seleccione una muestra de servidores (Microsoft Windows y Unix/Linux) a través de una muestra representativa de comerciantes y proveedores de servicios alojados y realice de A.1.1 a A.1.4 a continuación.			
A.1.1 Asegúrese de que cada entidad sólo lleve a cabo procesos con acceso al entorno de datos de titulares de tarjetas de la entidad.	**A.1.1** Si un proveedor de hosting compartido permite a las entidades (por ejemplo, comerciantes o proveedores de servicios) ejecutar sus propias aplicaciones, verifique que estos procesos de aplicación se ejecuten utilizando la ID única de la entidad. Por ejemplo: ▪ Ninguna entidad del sistema puede utilizar una ID de usuario de servidor Web compartida. ▪ Todas las secuencias de comandos CGI utilizadas por una entidad se deben crear y ejecutar como ID de usuario única de la entidad.			

Requisitos	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
A.1.2 Restrinja el acceso y los privilegios de cada entidad para que sólo contengan el entorno de datos de titulares de tarjetas.	**A.1.2.a** Verifique que la ID de usuario de cualquier proceso de aplicación no sea un usuario con privilegios (raíz/admin).			
	A.1.2.b Verifique que cada entidad (comerciante, proveedor de servicios) haya leído, escrito o ejecute permisos sólo para los archivos y directorios que tiene o para los archivos necesarios para el sistema (restringidos mediante permisos de sistema de archivos, listas de control de acceso, chroot, jailshell, etc.). IMPORTANTE: Los archivos de una entidad no deben compartirse de forma grupal.			
	A.1.2.c Verifique que los usuarios de una entidad no tengan acceso de escritura a archivos binarios compartidos del sistema.			
	A.1.2.d Verifique que la visualización de las entradas del registro se restrinjan a la entidad propietaria.			
	A.1.2.e Para asegurarse de que ninguna entidad pueda acaparar los recursos del servidor y aprovecharse de las vulnerabilidades (por ejemplo, error, carrera y condiciones de reinicio que tienen como resultado, por ejemplo, desbordamientos de buffer), verifique que se apliquen las restricciones para el uso de estos recursos del sistema: ▪ Espacio en disco ▪ Ancho de banda ▪ Memoria ▪ CPU			
A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos de titulares de tarjetas de cada entidad, así como también que cumplan con el Requisito 10 de las PCI DSS.	**A.1.3.a** Verifique que el proveedor de hosting compartido haya habilitado los registros de la siguiente manera para cada comerciante y entorno de proveedor de servicios: ▪ Los registros se habilitan para aplicaciones comunes de terceros. ▪ Los registros están activos de forma predeterminada. ▪ Los registros están disponibles para la revisión de la entidad propietaria. ▪ La ubicación de los registros se comunica con claridad a la entidad propietaria.			

Requisitos	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
A.1.4 Habilite los procesos para proporcionar una investigación forense oportuna en caso de riesgos para un comerciante o proveedor de servicios alojado.	**A.1.4** Verifique que el proveedor de hosting compartido cuente con políticas escritas que proporcionen una investigación forense oportuna de los servidores relacionados en caso de riesgos.			

Anexo B: Controles de compensación

Los controles de compensación se pueden tener en cuenta para la mayoría de los requisitos de las PCI DSS cuando una entidad no puede cumplir con un requisito explícitamente establecido, debido a los límites comerciales legítimos técnicos o documentados, pero pudo mitigar el riesgo asociado con el requisito de forma suficiente, mediante la implementación de otros controles, o controles de compensación.

Los controles de compensación deben cumplir con los siguientes criterios:

1. Cumplir con el propósito y el rigor del requisito original de las PCI DSS.
2. Proporcionar un nivel similar de defensa, tal como el requisito original de PCI DSS, de manera que el control de compensación compense el riesgo para el cual se diseñó el requisito original de las PCI DSS. (Consulte Exploración de PCI DSS para obtener el propósito de cada requisito de PCI DSS.)
3. Conozca en profundidad otros requisitos de las PCI DSS. (El simple cumplimiento con otros requisitos de las PCI DSS no constituye un control de compensación).

   Al evaluar exhaustivamente los controles de compensación, considere lo siguiente:

   Nota: los puntos a) a c) que aparecen a continuación son sólo ejemplos. El asesor que realiza la revisión de las PCI DSS debe revisar y validar si los controles de compensación son suficientes. La eficacia de un control de compensación depende de los aspectos específicos del entorno en el que se implementa el control, los controles de seguridad circundantes y la configuración del control. Las empresas deben saber que un control de compensación en particular no resulta eficaz en todos los entornos.

   a) Los requisitos de las PCI DSS NO SE PUEDEN considerar controles de compensación si ya fueron requisito para el elemento en revisión. Por ejemplo, las contraseñas para el acceso administrativo sin consola se deben enviar cifradas para mitigar el riesgo de que se intercepten contraseñas administrativas de texto claro. Una entidad no puede utilizar otros requisitos de contraseña de las PCI DSS (bloqueo de intrusos, contraseñas complejas, etc.) para compensar la falta de contraseñas cifradas, puesto que esos otros requisitos de contraseña no mitigan el riesgo de que se intercepten las contraseñas de texto claro. Además, los demás controles de contraseña ya son requisitos de las PCI DSS para el elemento en revisión (contraseñas).

   b) Los requisitos de las PCI DSS SE PUEDEN considerar controles de compensación si se requieren para otra área, pero no son requisito para el elemento en revisión. Por ejemplo, la autenticación de dos factores es un requisito de las PCI DSS para el acceso remoto. La autenticación de dos factores *desde la red interna* también se puede considerar un control de compensación para el acceso administrativo sin consola cuando no se puede admitir la transmisión de contraseñas cifradas. La autenticación de dos factores posiblemente sea un control de compensación aceptable si; (1) cumple con el propósito del requisito original al abordar el riesgo de que se intercepten las contraseñas administrativa de texto claro y (2) está adecuadamente configurada y en un entorno seguro.

   c) Los requisitos existentes de la PCI DSS se pueden combinar con nuevos controles para convertirse en un control de compensación. Por ejemplo, si una empresa no puede dejar ilegibles los datos de los titulares de tarjetas según el requisito 3.4 (por ejemplo, mediante cifrado), un control de compensación podría constar de un dispositivo o combinación de dispositivos, aplicaciones y controles que aborden lo siguiente: (1) segmentación interna de la red; (2) filtrado de dirección IP o MAC y (3) autenticación de dos factores desde la red interna.
4. Sea cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS

El asesor debe evaluar por completo los controles de compensación durante cada evaluación anual de PCI DSS para validar que cada control de compensación aborde de forma correcta el riesgo para el cual se diseñó el requisito original de PCI DSS, según los puntos 1 a 4 anteriores. Para mantener el cumplimiento, se deben aplicar procesos y controles para garantizar que los controles de compensación permanezcan vigentes después de completarse la evaluación.

Anexo C: Hoja de trabajo de controles de compensación

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el cual se utilicen controles de compensación para cumplir con un requisito de PCI DSS. Tenga en cuenta que los controles de compensación también se deben documentar en el Informe sobre cumplimiento en la sección de requisitos de PCI DSS correspondiente.

Nota: *Sólo las empresas que han llevado a cabo un análisis de riesgos y que tienen limitaciones legítimas tecnológicas o documentadas pueden considerar el uso de controles de compensación para lograr el cumplimiento.*

Número de requisito y definición:

	Información requerida	Explicación
1. Limitaciones	Enumere las limitaciones que impiden el cumplimiento con el requisito original.	
2. Objetivo	Defina el objetivo del control original; identifique el objetivo con el que cumple el control de compensación.	
3. Riesgo identificado	Identifique cualquier riesgo adicional que imponga la falta del control original.	
4. Definición de controles de compensación	Defina controles de compensación y explique de qué manera identifican los objetivos del control original y el riesgo elevado, si es que existe alguno.	
5. Validación de controles de compensación	Defina de qué forma se validaron y se probaron los controles de compensación.	
6. Mantenimiento	Defina los procesos y controles que se aplican para mantener los controles de compensación.	

Hoja de trabajo de controles de compensación – Ejemplo completo

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito indicado como "implementado" a través de los controles de compensación.

Número de requisito: *8.1¿Todos los usuarios se identifican con un nombre de usuario único antes de permitirles tener acceso a componentes del sistema y a datos de titulares de tarjetas?*

	Información requerida	Explicación
1. Limitaciones	Enumere las limitaciones que impiden el cumplimiento con el requisito original.	*La empresa XYZ emplea servidores Unix independientes sin LDAP. Como tales, requieren un inicio de sesión "raíz". Para la empresa XYZ no es posible gestionar el inicio de sesión "raíz" ni es factible registrar toda la actividad "raíz" de cada usuario.*
2. Objetivo	Defina el objetivo del control original; identifique el objetivo con el que cumple el control de compensación.	*El objetivo del requisito de inicios de sesión únicos es doble. En primer lugar, desde el punto de vista de la seguridad, no se considera aceptable compartir las credenciales de inicio de sesión. En segundo lugar, el tener inicios de sesión compartidos hace imposible establecer de forma definitiva a la persona responsable de una acción en particular.*
3. Riesgo identificado	Identifique cualquier riesgo adicional que imponga la falta del control original.	*Al no garantizar que todos los usuarios cuenten con una ID única y se puedan rastrear, se introduce un riesgo adicional en el acceso al sistema de control.*
4. Definición de controles de compensación	Defina controles de compensación y explique de qué manera identifican los objetivos del control original y el riesgo elevado, si es que existe alguno.	*La empresa XYZ requerirá que todos los usuarios inicien sesión en servidores desde sus escritorios mediante el comando SU. SU permite que el usuario obtenga acceso a la cuenta "raíz" y realice acciones dentro de la cuenta "raíz", aunque puede iniciar sesión en el directorio de registros SU. De esta forma, las acciones de cada usuario se pueden rastrear mediante la cuenta SU.*
5. Validación de controles de compensación	Defina de qué forma se validaron y se probaron los controles de compensación.	*La empresa XYZ demuestra al asesor que el comando SU que se ejecuta y las personas que utilizan el comando se encuentran conectados e identifica que la persona realiza acciones con privilegios raíz.*
6. Mantenimiento	Defina los procesos y controles que se aplican para mantener los controles de compensación.	*La empresa XYZ documenta procesos y procedimientos, y garantiza que no se cambie, se modifique, ni se elimine la configuración de SU y se permita que usuarios ejecuten comandos raíz sin que se los pueda rastrear o registrar.*

Anexo D: Declaración de cumplimiento – Comerciantes

Industria de Tarjetas de Pago (PCI)
Normas de Seguridad de Datos

Declaración de cumplimiento de evaluación in situ - Comerciantes

Versión 1.2.1

Julio de 2009

Instrucciones para la presentación

El presente documento debe ser completado por un Asesor de Seguridad Certificado (QSA) o comerciante (si la auditoría interna del comerciante realiza la validación) como declaración del estado de cumplimiento del comerciante con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Complete todas las secciones correspondientes y envíe al adquiriente o a la marca de pago solicitante.

Parte 1. Información de la empresa sobre el Asesor de Seguridad Certificado						
Nombre de la empresa:						
Nombre de contacto del QSA principal:			Cargo:			
N.º de teléfono:			Dirección de correo electrónico:			
Dirección comercial:			Ciudad:			
Estado/Provincia:		País:		Código postal:		
URL:						

Parte 2. Información sobre la organización del comerciante						
Nombre de la empresa:			Nombre(s) comercial(es) (DBA):			
Nombre de contacto:			Cargo:			
N.º de teléfono:			Dirección de correo electrónico:			
Dirección comercial:			Ciudad:			
Estado/Provincia:		País:		Código postal:		
URL:						

Parte 2a. Tipo de actividad comercial del comerciante (marque todo lo que corresponda)

☐ Comercio minorista ☐ Telecomunicaciones ☐ Tienda de comestibles y supermercados

☐ Petróleo ☐ Comercio electrónico ☐ Pedidos por correo/teléfono

☐ Viajes y entretenimientos ☐ Otros (especifique):

Enumere las instalaciones y ubicaciones incluidas en la revisión de PCI DSS:

Parte 2b. Relaciones

¿Su empresa tiene relación con uno o más agentes externos (por ejemplo, empresas de puertas de enlace y Web hosting, agentes de reservas aéreas, agentes de programas de lealtad, etc.)? ☐ Sí ☐ No

¿Su empresa tiene relación con más de un adquiriente? ☐ Sí ☐ No

Parte 2c. Procesamiento de transacciones

Aplicación de pago en uso: Versión de la aplicación de pago:

Parte 3. Validación de las PCI DSS

Según los resultados observados en el informe sobre cumplimiento de fecha *(date of ROC)*, *(QSA Name/Merchant Name)* afirma que el siguiente estado corresponde al estado de cumplimiento de la entidad identificada en la Parte 2 del presente documento al *(date)* (marque una opción):

☐ **Conforme:** Todos los requisitos del informe sobre cumplimiento tienen la marca "implementado[4]", y el Proveedor Aprobado de Escaneo de PCI SSC completó un análisis aprobado,*(ASV Name)* por consiguiente *(Merchant Company Name)*ha demostrado total cumplimiento con las *(insert version number)*.

☐ **No conforme:** Algunos requisitos del informe sobre cumplimiento tienen la marca "no implementado", lo que tiene como resultado una calificación general de **NO CONFORME**, **o bien** el Proveedor Aprobado de Escaneo de PCI SSC no ha completado un análisis aprobado, y por consiguiente*(Merchant Company Name)* no ha demostrado total cumplimiento con las PCI DSS.

Fecha objetivo para el cumplimiento:

Una entidad que envía el presente formulario con el estado No conforme posiblemente deba completar el Plan de acción de la Parte 4 de este documento. *Consulte con su adquiriente o la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

Parte 3a. Confirmación del estado de cumplimiento

Confirmación de QSA/comerciante:

☐	El informe sobre cumplimiento se completó de acuerdo con los *Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad*, versión *(insert version number)*, y de conformidad con las instrucciones allí consideradas.
☐	Toda la información que aparece dentro del informe de cumplimiento antes mencionado y en esta declaración muestran los resultados de la evaluación de manera equitativa en todos sus aspectos sustanciales.
☐	El comerciante ha confirmado con el proveedor de la aplicación de pago que su aplicación de pago no almacena los datos de autenticación confidenciales después de la autorización.
☐	El comerciante ha leído las PCI DSS y reconoce que deben cumplir plenamente con las PCI DSS en todo momento.
☐	No existe evidencia de almacenamiento de datos de banda magnética (es decir, ninguna pista)[5], datos de CAV2, CVC2, CID, o CVV2[6], ni datos de PIN[7] después de encontrarse la autorización de la transacción en TODOS los sistemas revisados durante la presente evaluación.

Parte 3b. Agradecimientos del QSA y el comerciante

Firma del QSA principal ↑	***Fecha:***
Nombre del QSA principal:	***Cargo:***

Firma del Oficial Ejecutivo del comerciante ↑	***Fecha:***
Nombre del Oficial Ejecutivo del comerciante:	***Cargo:***

[4] Los resultados "Implementado" deben incluir los controles de compensación revisados por la auditoría interna del QSA/comerciante. Si se determina que los controles de compensación mitigan el riesgo asociado con el requisito de manera suficiente, el QSA debe marcar el requisito como "implementado".

[5] Datos codificados en la banda magnética que se utilizan para realizar la autorización durante una transacción con tarjeta presente. Es posible que las entidades no retengan todos los datos de banda magnética después de la autorización de la transacción. Los únicos elementos de datos de pistas que se pueden retener son: el número de cuenta, la fecha de vencimiento y el nombre.

[6] El valor de tres o cuatro dígitos impreso en el panel de firma o en el anverso de la tarjeta de pago que se utiliza para verificar las transacciones con tarjeta ausente (CNP).

[7] El número de identificación personal introducido por el titular de la tarjeta durante una transacción con tarjeta presente y/o el bloqueo del PIN cifrado presente dentro del mensaje de la transacción.

Parte 4. Plan de acción para el estado de no conformidad

Seleccione el "Estado de cumplimiento" adecuado para cada requisito. Si la respuesta a cualquier requisito es “No”, debe proporcionar la fecha en la que la empresa cumplirá con el requisito y una breve descripción de las medidas que se tomarán para cumplirlo. *Consulte con su adquiriente o la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

Requisito PCI	Descripción	Estado de cumplimiento (Seleccione uno)	Fecha de la recuperación y acciones (si el estado de cumplimiento es “No”)
1	Instale y mantenga una configuración de firewall para proteger los datos de titulares de tarjetas.	☐Sí ☐ No	
2	No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad.	☐Sí ☐ No	
3	Proteja los datos del titular de la tarjeta que fueron almacenados.	☐Sí ☐ No	
4	Cifre la transmisión de datos de titulares de tarjetas a través de redes abiertas y públicas.	☐Sí ☐ No	
5	Utilice y actualice con regularidad un software de antivirus.	☐Sí ☐ No	
6	Desarrolle y mantenga sistemas y aplicaciones seguros.	☐Sí ☐ No	
7	Restrinja el acceso a datos de titulares de tarjetas sólo a la necesidad de conocimiento de la empresa.	☐Sí ☐ No	
8	Asigne una ID única a cada persona que tenga acceso a equipos.	☐Sí ☐ No	
9	Restrinja el acceso físico a datos de titulares de tarjetas.	☐Sí ☐ No	
10	Rastree y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.	☐Sí ☐ No	
11	Pruebe con regularidad los sistemas y procesos de seguridad.	☐Sí ☐ No	
12	Mantenga una política que aborde la seguridad de la información.	☐Sí ☐ No	

Anexo E: Declaración de cumplimiento – Proveedores de servicios

Industria de Tarjetas de Pago (PCI)
Normas de Seguridad de Datos

Declaración de cumplimiento de evaluación in situ - Proveedores de servicios

Versión 1.2.1

Julio de 2009

Instrucciones para la presentación

El Asesor de Seguridad Calificado (QSA) y el proveedor de servicios deben completar el presente documento como declaración del estado de cumplimiento del proveedor de servicios respecto de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Complete todas las secciones correspondientes y envíe a la marca de pago solicitante.

Parte 1. Información de la empresa sobre el Asesor de Seguridad Certificado							
Nombre de la empresa:							
Nombre de contacto del QSA principal:				Cargo:			
N.º de teléfono:				Dirección de correo electrónico:			
Dirección comercial:				Ciudad:			
Estado/Provincia:		País:			Código postal:		
URL:							

Parte 2. Información sobre la organización del proveedor de servicios							
Nombre de la empresa:				Nombre(s) comercial(es) (DBA):			
Nombre de contacto:				Cargo:			
N.º de teléfono:				Dirección de correo electrónico:			
Dirección comercial:				Ciudad:			
Estado/Provincia:		País:			Código postal:		
URL:							

Parte 2a. Servicios prestados (marque todo lo que corresponda)

☐ Autorización	☐ Programas de lealtad	☐ 3-D Secure Access Control Server
☐ Switching	☐ IPSP (Comercio electrónico)	☐ Transacciones con proceso de banda magnética
☐ Pasarela de pago	☐ Compensación y liquidación	☐ Proceso de transacciones por correo/teléfono
☐ Hosting	☐ Procesamiento de emisión	☐ Otros (especifique):

Enumere las instalaciones y ubicaciones incluidas en la revisión de PCI DSS:

Parte 2b. Relaciones

¿Su empresa tiene relación con uno o más proveedores de servicios externos (por ejemplo, empresas de puertas de enlace y Web hosting, agentes de reservas aéreas, agentes de programas de lealtad, etc.)? ☐ Sí ☐ No

Parte 2c. Procesamiento de transacciones

¿De qué forma y en qué capacidad almacena, procesa y/o transmite su empresa los datos de titulares de tarjetas?

Aplicación de pago en uso:	*Versión de la aplicación de pago:*

Parte 3. Validación de las PCI DSS

Según los resultados observados en el informe sobre cumplimiento de fecha *(date of ROC)*, *(QSA Name)* afirma que el siguiente estado corresponde al estado de cumplimiento de la entidad identificada en la Parte 2 del presente documento al *(date)* (marque una opción):

☐ **Conforme:** Todos los requisitos del informe sobre cumplimiento tienen la marca "implementado[8]", y el Proveedor Aprobado de Escaneo de PCI SSC completó un análisis aprobado,*(ASV Name)* por consiguiente *(Service Provider Name)*ha demostrado total cumplimiento con las *(insert version number)*.

☐ **No conforme:** Algunos requisitos del informe sobre cumplimiento tienen la marca "no implementado", lo que tiene como resultado una calificación general de **NO CONFORME**, **o bien** el Proveedor Aprobado de Escaneo de PCI SSC no ha completado un análisis aprobado, y por consiguiente*(Service Provider Name)* no ha demostrado total cumplimiento con las PCI DSS.

Fecha objetivo para el cumplimiento:

Una entidad que envía el presente formulario con el estado No conforme posiblemente deba completar el Plan de acción de la Parte 4 de este documento. *Consulte con la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

Parte 3a. Confirmación del estado de cumplimiento

Confirmación del QSA y el proveedor de servicios:

☐	El informe sobre cumplimiento se completó de acuerdo con los *Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad*, versión *(insert version number)*, y de conformidad con las instrucciones allí consideradas.
☐	Toda la información que aparece dentro del informe de cumplimiento antes mencionado y en esta declaración muestran los resultados de la evaluación de manera equitativa en todos sus aspectos sustanciales.
☐	El proveedor de servicios ha leído las PCI DSS y reconoce que deben cumplir plenamente con las PCI DSS en todo momento.
☐	No existe evidencia de almacenamiento de datos de banda magnética (es decir, ninguna pista)[9], datos de CAV2, CVC2, CID, o CVV2[10], ni datos de PIN[11] después de encontrarse la autorización de la transacción en TODOS los sistemas revisados durante la presente evaluación.

Parte 3b. Agradecimientos del QSA y el proveedor de servicios

Firma del QSA principal ↑	***Fecha:***
Nombre del QSA principal:	***Cargo:***

Firma del Oficial Ejecutivo del proveedor de servicios ↑	***Fecha:***
Nombre del Oficial Ejecutivo del proveedor de servicios:	***Cargo:***

[8] Los resultados "Implementado" deben incluir los controles de compensación revisados por el QSA. Si se determina que los controles de compensación mitigan el riesgo asociado con el requisito de manera suficiente, el QSA debe marcar el requisito como "implementado".

[9] Datos codificados en la banda magnética que se utilizan para realizar la autorización durante una transacción con tarjeta presente. Es posible que las entidades no retengan todos los datos de banda magnética después de la autorización de la transacción. Los únicos elementos de datos de pistas que se pueden retener son: el número de cuenta, la fecha de vencimiento y el nombre.

[10] El valor de tres o cuatro dígitos impreso en el panel de firma o en el anverso de la tarjeta de pago que se utiliza para verificar las transacciones con tarjeta ausente (CNP).

[11] El número de identificación personal introducido por el titular de la tarjeta durante una transacción con tarjeta presente y/o el bloqueo del PIN cifrado presente dentro del mensaje de la transacción.

Parte 4. Plan de acción para el estado de no conformidad

Seleccione el "Estado de cumplimiento" adecuado para cada requisito. Si la respuesta a cualquier requisito es “No”, debe proporcionar la fecha en la que la empresa cumplirá con el requisito y una breve descripción de las medidas que se tomarán para cumplirlo. *Consulte con la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

Requisito PCI	Descripción	Estado de cumplimiento (Seleccione uno)	Fecha de la recuperación y acciones (si el estado de cumplimiento es “No”)
1	Instale y mantenga una configuración de firewall para proteger los datos de titulares de tarjetas.	☐Sí ☐ No	
2	No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad.	☐Sí ☐ No	
3	Proteja los datos del titular de la tarjeta que fueron almacenados.	☐Sí ☐ No	
4	Cifre la transmisión de datos de titulares de tarjetas a través de redes abiertas y públicas.	☐Sí ☐ No	
5	Utilice y actualice con regularidad un software de antivirus.	☐Sí ☐ No	
6	Desarrolle y mantenga sistemas y aplicaciones seguros.	☐Sí ☐ No	
7	Restrinja el acceso a datos de titulares de tarjetas sólo a la necesidad de conocimiento de la empresa.	☐Sí ☐ No	
8	Asigne una ID única a cada persona que tenga acceso a equipos.	☐Sí ☐ No	
9	Restrinja el acceso físico a datos de titulares de tarjetas.	☐Sí ☐ No	
10	Rastree y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.	☐Sí ☐ No	
11	Pruebe con regularidad los sistemas y procesos de seguridad.	☐Sí ☐ No	
12	Mantenga una política que aborde la seguridad de la información.	☐Sí ☐ No	

Anexo F: Revisiones de PCI DSS — Alcance y selección de muestras