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

Requisitos y procedimientos de evaluación de seguridad

Versión 2.0

Octubre de 2010

Modificaciones realizadas a los documentos

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 las PCI DSS versión 1.1 a 1.2).	
Julio de 2009	*1.2.1*	*Agregar la oración que se eliminó incorrectamente entre las 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 de modo que diga "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*
Octubre de 2010	*2.0*	*Actualizar e implementar cambios de la versión 1.2.1. Para obtener los detalles, consulte "*PCI DSS - Resumen de cambios de las PA-DSS versión 1.2.1 a 2.0."	

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. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos. A continuación, encontrará una descripción general de los 12 requisitos de las PCI DSS.

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

Desarrollar y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta 2. No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	5. Utilice y actualice con regularidad los programas o software antivirus 6. Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa 8. Asignar una ID exclusiva a cada persona que tenga acceso por computador 9. Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas 11. Pruebe con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	12. Mantenga una política que aborde la seguridad de la información para todo el personal

Este documento, *Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad*, combina los 12 requisitos de las PCI DSS y los procedimientos de prueba correspondientes en una herramienta de evaluación de seguridad. Se desarrolló para utilizarse durante las evaluaciones de cumplimiento con las PCI DSS como parte del proceso de validación de una entidad. Las siguientes secciones

proporcionan directrices detalladas y mejores prácticas para ayudar a las entidades a estar preparadas para realizar una evaluación de las PCI DSS y comunicar los resultados. Los requisitos de las PCI DSS y los procedimientos de prueba comienzan en la **página 19.**

El sitio web de las PCI Security Standards Council (PCI SSC) (www.pcisecuritystandards.org) contiene un número de recursos adicionales, incluidos:

- Declaración de cumplimiento
- *Navegación de las PCI DSS: Comprensión del objetivo de los requisitos*
- El *glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS*
- Preguntas frecuentes (FAQ)
- Suplementos informativos y directrices

***Nota**: Los suplementos informativos complementan las PCI DSS e identifican las consideraciones y recomendaciones adicionales para cumplir con los requisitos de las PCI DSS, las cuales no modifican ni eliminan ni sustituyen las PCI DSS ni ninguno de sus requisitos.*

Visite www.pcisecuritystandards.org para obtener más información.

Información sobre la aplicabilidad de las PCI DSS

Las PCI DSS se aplican donde sea que se almacenen, procesen o transmitan datos de cuentas. *Los datos de cuentas* constan de los *datos de los titulares de tarjetas* más *datos confidenciales de autenticación,* como se detalla a continuación:

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

El número de cuenta principal es el factor que define la aplicabilidad de los requisitos de las PCI DSS. 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 ni procesa ni transmite, no se aplican los requisitos de las PCI DSS.

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

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

La siguiente tabla 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 y de que esos datos deban estar protegidos. Esta tabla no es exhaustiva, sino que tiene por objeto ilustrar los distintos tipos de requisitos que se aplican a cada elemento de datos.

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

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

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

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

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

Relación entre PCI DSS y PA-DSS

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

Los requisitos de las Normas de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS) se derivan de los *Requisitos de las PCI DSS y de los Procedimiento de Evaluación de Seguridad* (este documento). Las PA-DSS **Error! Hyperlink reference not valid.**detallan lo que debe poseer una aplicación de pago para facilitar el cumplimiento de las PCI DSS por parte de un cliente.

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

Algunas de las maneras en que las aplicaciones de pago pueden impedir el cumplimiento:

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

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

Tenga en cuenta lo siguiente en relación con la aplicabilidad de las PA-DSS:

- Las PA-DSS ***sí*** se aplican a las aplicaciones de pago que los proveedores de software generalmente venden e instalan "en forma estándar" sin demasiada personalización.
- Las PA-DSS ***no*** se aplican a aplicaciones de pago desarrolladas por comerciantes y proveedores de servicios si sólo se utilizan internamente (no se venden, no se distribuyen ni se otorgan bajo licencia a terceros), dado que estas aplicaciones de uso interno deberían estar sujetas al cumplimiento normal de las PCI DSS por parte de los comerciantes o proveedores de servicios.

Para obtener una orientación detallada sobre cómo determinar si las PA-DSS rigen una aplicación de pago determinada, consulte los requisitos de las PA-DSS y los Procedimientos de Evaluación de Seguridad, que están disponibles en www.pcisecuritystandards.org.

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

Los requisitos de seguridad de las PCI DSS se aplican a todos los componentes del sistema. En el contexto de las PCI DSS, los "componentes del sistema" se definen como cualquier componente de red, servidor o aplicación que esté incluida en el entorno de los datos del titular de la tarjeta o que esté conectado a éste. Los “componentes del sistema” también incluyen cualesquiera componentes de virtualización tales como máquinas virtuales, interruptores/routers virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores. El entorno de los datos de los titulares de tarjetas consta de personas, procesos y tecnología que almacenan, procesan o transmiten datos de titulares de tarjetas o 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 personalizadas, incluidas las aplicaciones internas y externas (como Internet).

El primer paso de una evaluación de las PCI DSS es determinar con exactitud el alcance de la revisión. Por lo menos una vez al año y antes de la evaluación anual, la entidad evaluada debería confirmar la exactitud del alcance de las PCI DSS al identificar todas las ubicaciones y flujos de datos de titulares de tarjetas y al asegurar que se incluyan en el alcance de las PCI DSS. Para confirmar la exactitud e idoneidad del alcance de las PCI DSS, realice lo siguiente:

- La entidad evaluada identifica y documenta la existencia de todos los datos de los titulares de tarjetas en su entorno, con la finalidad de verificar que no haya datos de titulares de tarjetas fuera del entorno de los datos de los titulares de tarjetas (CDE) actualmente definido.
- Una vez que se hayan identificado y documentado todas las ubicaciones de los datos de los titulares de tarjetas, la entidad utiliza los resultados para verificar que el alcance de las PCI DSS sea apropiado (por ejemplo, los resultados pueden ser un diagrama o un inventario de ubicaciones de datos de titulares de tarjetas).
- La entidad considera que todos los datos de titulares de tarjetas encontrados están dentro del alcance de la evaluación de las PCI DSS y forman parte del CDE, a menos que dichos datos se eliminen o migren/consoliden en el CDE actualmente definido.
- La entidad retiene la documentación que demuestre los resultados y cómo se confirmó el alcance de las PCI DSS para la revisión por parte de los asesores y/o como referencia durante la actividad anual de la siguiente confirmación de alcance de las PCI SCC.

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 de una entidad no constituye un requisito de las PCI DSS. Sin embargo, se recomienda ampliamente como un método que puede disminuir:

- El alcance de la evaluación de las PCI DSS
- El costo de la evaluación de las PCI DSS
- El costo y la dificultad de la implementación y del mantenimiento de los controles de las PCI DSS
- 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 PCI DSS. La segmentación de red se puede alcanzar mediante diversos medios físicos o lógicos, tales como firewalls internos de red, routers con sólidas listas de control de acceso u otras tecnologías con la apropiada configuración que restrinjan el acceso a un segmento particular de la red.

Un prerrequisito importante para reducir el alcance del entorno de los datos del titular de la tarjeta es la comprensión de las necesidades del negocio y de los procesos relacionados con el almacenamiento, el procesamiento o la transmisión 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 de negocio 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 PCI DSS, el asesor debe verificar que la segmentación sea adecuada para reducir el alcance de la evaluación. De la manera más detallada posible, la adecuada segmentación de red aísla los sistemas que almacenan, procesan o transmiten 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 enormemente y depende de ciertas factores como la configuración de una red determinada, las tecnologías que se utilizan y otros controles que puedan implementarse.

Anexo D: La Segmentación y muestreo de instalaciones de negocios/Componentes de sistemas proporciona más información sobre el efecto de la segmentación y el muestreo de la red sobre el alcance de una evaluación de las PCI DSS.

Medios inalámbricos

Si se utiliza tecnología inalámbrica para almacenar, procesar o transmitir datos del titular de la tarjeta (por ejemplo, transacciones de puntos de venta, “line-busting”) o si hay una red de acceso local inalámbrica (WLAN) 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 prueba para entornos inalámbricos de las PCI DSS (por ejemplo, requisitos 1.2.3, 2.1.1 y 4.1.1). Recomendamos que antes de implementar la tecnología inalámbrica, una entidad 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/tercerización

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 del entorno de datos del titular de la tarjeta.

Los comerciantes o proveedores de servicio pueden utilizar un proveedor de servicios externo para almacenar, procesar o transmitir datos del titular de la tarjeta en su nombre, o para administrar componentes como routers, firewalls, bases de datos, seguridad física y/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 tercerizan el almacenamiento, el procesamiento o la transmisión 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 servicios 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 opciones para validar el cumplimiento:

1) Pueden realizar una evaluación de las PCI DSS por cuenta propia y proporcionar evidencia a sus clientes a fin de demostrar el cumplimiento; o

2) Si no realizan la evaluación de las PCI DSS por cuenta propia, deberán solicitar la revisión de sus servicios durante el curso de cada una de las evaluaciones de las PCI DSS 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, Detalle sobre el entorno bajo revisión", de la sección "Instrucciones y contenido del informe de cumplimiento", que se encuentra abajo.

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

Muestreo de instalaciones de negocios/Componentes de sistemas

El muestreo no es un requisito de las PCI DSS. Sin embargo, después de considerar el alcance global y la complejidad del entorno que se está evaluando, el asesor puede seleccionar de manera independiente muestras de instalaciones de negocios/componentes del sistema a fin de evaluar los requisitos de las PCI DSS. Estas muestras se deben definir primero para instalaciones de negocios y luego para los componentes del sistema dentro de cada instalación del negocio seleccionada. Las muestras deben constituir una selección representativa de todos los tipos y las ubicaciones de las instalaciones del negocio, así como de los tipos de los componentes del sistema dentro de las instalaciones del negocio seleccionadas. Las muestras deben ser suficientemente grandes para proporcionar al asesor la seguridad de que los controles se implementaron de la manera esperada.

El muestreo de las instalaciones del negocio/componentes del sistema para una evaluación no reduce el alcance del entorno de los datos de los titulares de tarjetas o la aplicabilidad de los requisitos de las PCI DSS. Independientemente de si se utiliza o no el muestreo, los requisitos de las PCI DSS se aplican al entorno de datos de los titulares de tarjetas en su totalidad. Si se utiliza muestreo, cada muestra se debe evaluar en función de todos los requisitos de las PCI DSS aplicables. El muestreo de los requisitos de las PCI DSS en sí no está permitido.

Entre las instalaciones de negocios se incluyen, a modo de ejemplo: oficinas corporativas, tiendas, franquicias, instalaciones de procesamiento, centros de datos y otros tipos de instalación en diferentes ubicaciones. Las muestras deben incluir componentes de sistemas dentro de cada instalación del negocio seleccionada. Por ejemplo, por cada instalación del negocio seleccionada, incluya distintos sistemas operativos, funciones y aplicaciones que se apliquen al área en evaluación.

Por ejemplo, en cada instalación del negocio, el asesor podría definir una muestra para incluir 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 7 o Sun 10), entonces la muestra deberá incluir una variedad de aplicaciones (por ejemplo, servidores de base de datos, servidores de Web y servidores de transferencia de datos).

Al seleccionar muestras de las instalaciones del negocio/componentes del sistema, los asesores deberán tener en cuenta lo siguiente:

- Si están implementados procesos y controles estándares y centralizados de seguridad y operativos para las PCI DSS que garanticen uniformidad y que debe seguir cada instalación del negocio/componente del sistema, la muestra puede ser más pequeña que si no hubiera procesos/controles estándares implementados. La muestra debe ser suficientemente grande para proporcionar al asesor la garantía razonable de que todas las instalaciones del negocio/componentes del sistema se configuraron según los procesos estándares.
- Si no está implementado más de un tipo de proceso operativo y/o de seguridad estándar (por ejemplo, para diferentes tipos de instalaciones del negocio/componentes del sistema), la muestra debe ser suficientemente grande para incluir las instalaciones del negocio/componentes del sistema asegurados con cada tipo de proceso.
- Si no están implementados procesos/controles de PCI DSS estándares y cada instalación del negocio/componente del sistema se administra a través de procesos no estándares, la muestra debe ser más grande para que el asesor pueda estar seguro de que cada instalación del negocio/componente del sistema implementó los requisitos de las PCI DSS de manera apropiada.

Para cada instancia donde se hayan utilizado muestras, el asesor debe:

- Documente la justificación de la técnica de muestreo y el tamaño de la muestra,
- Documente y valide los procesos y controles de las PCI DSS estandarizados que se utilizan para determinar el tamaño de la muestra y
- Explique la manera como la muestra es apropiada y representativa de toda la población.

Consulte: Anexo D: Segmentación y muestreo de instalaciones de negocios/Componentes de sistemas.

Los asesores deben revalidar la justificación del muestreo para cada evaluación. Si se utiliza muestreo, se deben seleccionar diferentes muestras de instalaciones del negocio y componentes del sistema para cada evaluación.

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 PCI DSS.

Para obtener más detalles 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 la plantilla 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 rol de su negocio con las tarjetas de pago, que es la manera en la que almacenan, procesan o transmiten 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 rol 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 a la sección Alcance de la evaluación de este documento, e incluya lo siguiente:

- Documentar cómo el asesor validó la exactitud del alcance de las PCI DSS para la evaluación, incluidos:
  - Los métodos o proceso utilizados para identificar y documentar todas las existencias de datos de titulares de tarjetas
  - Cómo se evaluaron y documentaron los resultados
  - Cómo se verificó la efectividad y exactitud de los métodos utilizados
  - La validación por parte del asesor de que el alcance de la evaluación es exacto y apropiado.
- 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 PCI DSS, describa esa segmentación y la manera en la que el asesor validó la eficacia de la segmentación.
- Si durante la evaluación se utilizó muestreo, para cada conjunto de muestras seleccionado (de las instalaciones del negocio/componentes del sistema) lo siguiente documentar:
  - Población total
  - Cantidad de muestras
  - Base para la selección de muestras
  - Descripción de los procesos y controles operativos y de seguridad estandarizados de las PCI DSS utilizados para determinar el tamaño de la muestra y cómo se validaron los procesos/controles
  - La manera como la muestra es apropiada y representativa de toda la población
  - Descripción de toda ubicación o entorno que almacene, procese o transmita datos de titulares de tarjetas que se EXCLUYERON del alcance de la revisión y la razón por la que se excluyeron dichas ubicaciones/entornos
- Enumerar toda entidad en propiedad absoluta que requiera cumplimiento con las PCI DSS y aclarar si se revisan por separado o como parte de esta evaluación
- Enumerar toda entidad internacional que requiera cumplimiento con las PCI DSS y si se revisan por separado o como parte de esta evaluación
- Enumerar 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 PCI DSS utilizado para realizar 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 archivos y tablas que almacenan datos de titulares de tarjetas, respaldados por un inventario creado (u obtenido del cliente) 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 utilizan 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 otros terceros con los cuales la entidad comparte datos de titulares de tarjetas

  Nota: *Estas entidades están sujetas al Requisito 12.8 de las PCI DSS*).
- 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 verificar que la aplicación se implementó de forma tal y en un entorno que cumple con las PCI DSS y conforme a la *Guía de implementación de PA-DSS* del proveedor de la aplicación de pago.

  Nota: *La utilización de aplicaciones PA-DSS validadas no es requisito de las PCI DSS. Consulte a cada marca de pago por separado para comprender sus requisitos de cumplimiento de PA-DSS).*
- Lista de personas entrevistadas, sus organizaciones, cargos y temas discutidos
- Lista de la documentación revisada
- En el caso de las revisiones de proveedores de servicios 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.
- Plazo de la evaluación—especifique la duración y el período de tiempo de la evaluación
- Fecha del informe

5. Resultados del análisis trimestral

- Resuma los resultados de los últimos cuatro análisis trimestrales del ASV en el Resumen ejecutivo y en los comentarios del Requisito 11.2.2.

  Nota: *Para determinar el cumplimiento de las PCI DSS inicial, no se requiere que se deban completar cuatro análisis trimestrales satisfactorios si el asesor verifica:*

  1) *Que el resultado del último análisis fue satisfactorio,*
  2) *Que la entidad haya documentado las políticas y los procedimientos que requieren la continuación de los análisis trimestrales y*
  3) *Que todas las vulnerabilidades observadas en el análisis inicial se hayan corregido, lo cual se comprobará después de otro análisis.*

  En el caso de los años siguientes a la revisión inicial de las PCI DSS, deben obtenerse cuatro análisis trimestrales aprobados.

- El análisis debe incluir todas las direcciones IP a las cuales se puede acceder externamente (Internet) que existan en la entidad, conforme a la *Guía del programa de Proveedores aprobados de análisis (AVS) de 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 PCI DSS y procedimientos de evaluación de seguridad detallados a los efectos de brindar detalladas descripciones y conclusiones de informes sobre cada requisito y subrequisito.
- Asegurarse de que todas las respuestas N/C se expliquen de manera clara.
- Revisar y documentar todo control de compensación que se utiliza para concluir que se implementó un control.

Para obtener más información sobre los controles de compensación, consulte la sección “Controles de compensación” que aparece más arriba y 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 haya corregido 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).

Pasos para completar el cumplimiento de las PCI DSS

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 PCI SSC completó los análisis aprobados de vulnerabilidad y solicítele pruebas al ASV de los análisis aprobados.
3. Complete la Declaración de cumplimiento para Proveedores de servicios o Comerciantes, según corresponda, en su totalidad. Las Declaraciones de cumplimiento están disponibles en el sitio web de las PCI SSC (www.pcisecuritystandards.org).
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 PCI DSS y procedimientos de evaluación de seguridad detallados

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

- **Requisitos de las PCI DSS**: esta columna define las normas de seguridad de datos y enumera los requisitos para alcanzar el cumplimiento de las PCI DSS, el cumplimiento se validará en comparación con estos requisitos.
- **Procedimientos de prueba:** esta columna muestra los procesos que el asesor debe seguir a los efectos de validar que los requisitos de las PCI DSS "se implementaron".
- **Implementados**: el asesor debe utilizar esta columna para proporcionar una breve descripción de los controles que se validaron como "implementados" para cada requisito, incluidas las descripciones de controles de los cuales se haya determinado su implementación como resultado de controles de compensación, o como resultado de un requisito "No aplicable".

  Nota: *Esta columna no debe utilizase para controles que no se hayan implementado ni para puntos sujetos a control 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. Para obtener instrucciones adicionales sobre informes en incumplimiento, consulte las Declaraciones de cumplimiento, disponibles en el sitio web de PCI SSC (www.pcisecuritystandards.org).
- **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. Todos los comentarios o las notas adicionales también se podrían incluir aquí.

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 que controlan el tráfico computarizado entre las redes (internas) y las redes no confiables (externas) de una entidad, así como el tráfico de entrada y salida a áreas más sensibles dentro de la red interna confidencial de una entidad. El entorno del titular de la tarjeta es un ejemplo de un área más confidencial dentro de la red confiable de una entidad.

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

Todos los sistemas debe estar protegidos 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 entre negocios 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.

Otros componentes del sistema pueden funcionar como firewall, siempre y cuando reúnan los requisitos mínimos correspondientes a firewalls, según se especifica en el Requisito 1. En las áreas donde se utilizan otros componentes del sistema dentro del entorno de datos de los titulares de tarjetas a fin de proporcionar la funcionalidad de firewall, estos dispositivos se deben incluir dentro del alcance y la evaluación del Requisito 1.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
1.1 Establezca normas de configuración para firewall y router que incluyan lo siguiente:	**1.1 Obtenga e inspeccione las normas de configuración del firewall y del router y otros documentos especificados más abajo para verificar que las normas se completaron. Complete lo siguiente:**			
1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers	**1.1.1** Verificar la existencia de un proceso formal para probar y aprobar 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 tarjetas, incluida toda red inalámbrica	**1.1.2.a** Verifique que exista un diagrama actualizado de la red (por ejemplo, uno que muestre los flujos de los datos de los titulares de tarjetas en la red) y que documenta todas las conexiones a los datos de los titulares de tarjetas, incluida toda red inalámbrica.			
	1.1.2.b Verifique 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	**1.1.3.a** Verifique que las normas 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
la zona de la red interna	**1.1.3.b** Verifique que el diagrama actual de la red concuerde con las normas de configuración de firewalls.			
1.1.4 Descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red	**1.1.4** Verifique que las normas de configuración del firewall y el router incluyan la descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red.			
1.1.5 Documentación y justificación de negocio para la utilización de todos los servicios, protocolos y puertos permitidos, incluida la documentación de funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros. Entre los servicios, protocolos o puertos no seguros se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP.	**1.1.5.a** Verifique que las normas de configuración de firewalls y routers incluyan una lista documentada de servicios, protocolos y 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 no seguros permitidos y verifique que sean necesarios y que las funciones de seguridad se documenten e implementen mediante la evaluación de las normas de configuración del firewall y del router y de los ajustes de cada servicio.			
1.1.6 Requisito de la revisión de las normas del firewall y el router, al menos, cada seis meses	**1.1.6.a** Verifique que las normas de configuración del firewall y el router soliciten la revisión de los conjuntos de reglas 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 reglas se revisen, al menos, cada seis meses.			
1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y todo componente del sistema en el entorno de los datos del titular de la tarjeta. ***Nota:*** *Una "red no confiable" es toda red que es externa a las redes que pertenecen a la entidad en evaluación y/o que excede la capacidad de control o administración de la entidad.*	**1.2** Examine la configuración de los firewalls y del router a los efectos de verificar 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:			
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad que sea necesaria en el entorno de datos del	**1.2.1.a** Verifique que el tráfico 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
titular de la tarjeta.	**1.2.1.b** Verifique que todo tráfico entrante o saliente se niegue de manera específica, 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** Verifique que los archivos de configuración del 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 o controlar (en caso de que ese tráfico fuera necesario para fines de negocio) todo tráfico desde el entorno inalámbrico hacia el entorno del titular de la tarjeta.	**1.2.3** Verifique 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 tráfico fuera necesario para fines de negocio) todo tráfico 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** Examine las configuraciones de firewalls y routers; incluido, a modo de ejemplo, el router de estrangulamiento de Internet, el router DMZ y el firewall, el segmento de titulares de tarjetas de DMZ, el router de perímetro y el segmento de la red interna del titular de la tarjeta, a fin de determinar que no exista acceso directo entre Internet y los componentes del sistema en el segmento de red interna del titular de la tarjeta, tal como se detalla más abajo.			
1.3.1 Implemente un DMZ para limitar el tráfico entrante sólo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	**1.3.1** Verifique que se haya implementado un DMZ para limitar el tráfico entrante sólo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.			
1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro del DMZ.	**1.3.2** Verifique que se restrinja el tráfico entrante de Internet a las direcciones IP dentro del DMZ.			
1.3.3 No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de	**1.3.3** Verifique que no se permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
la tarjeta.				
1.3.4 No permita que las direcciones internas pasen desde Internet al DMZ.	**1.3.4** Verifique que las direcciones internas no puedan pasar desde Internet al DMZ**.**			
1.3.5 No permita que llegue tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta a Internet.	**1.3.5** Verifique que se autorice de manera explícita el tráfico saliente proveniente del entorno de datos del titular de la tarjeta a Internet			
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** Verifique que el firewall realice una inspección completa (filtrado dinámico de paquetes). (Sólo se debe permitir la entrada de conexiones establecidas, y sólo si están asociadas a una sesión establecida anteriormente).			
1.3.7 Coloque los componentes del sistema que almacenan datos de titulares de tarjetas (como una base de datos) en una zona de red interna, segregada desde un DMZ y otras redes no confiables.	**1.3.7** Verifique que los componentes del sistema que almacenan datos de titulares de tarjetas (como una base de datos) se encuentren en una zona de red interna, segregada desde un DMZ y otras redes no confiables.			
1.3.8 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas. ***Nota:*** *Entre los métodos para ocultar direcciones IP se pueden incluir, a modo de ejemplo:* ▪ *Traducción de Dirección de Red (NAT)* ▪ *Ubicar servidores que contengan datos de titulares de tarjetas detrás de servidores proxy/firewalls o cachés de contenido,* ▪ *Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas,* ▪ *Uso interno del espacio de dirección RFC1918 en lugar de direcciones registradas.*	**1.3.8.a** Verifique que haya métodos implementados para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde redes internas a Internet.			
	1.3.8.b Verifique que no se autorice ninguna divulgación de direcciones IP privadas ni de información de enrutamiento a entidades externas.			

Requisitos de las PCI DSS	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** Verifique que toda computadora móvil y/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 Verifique que la organización configure el software de firewall personal a los efectos de detallar las normas 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 una entidad), 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 PCI DSS	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, incluidas, a modo de ejemplo, contraseñas, cadenas comunitarias de protocolo simple de administración de red (SNMP) y la eliminación de 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 verificar 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 transmiten datos del titular de la tarjeta, cambie los valores predeterminados proporcionados por los proveedores, incluidas, a modo de ejemplo, claves de cifrado inalámbricas predeterminadas, contraseñas y cadenas comunitarias SNMP.	**2.1.1** Verifique lo siguiente en relación con los valores de configuración para entornos inalámbricos:			
	2.1.1.a Verifique que las claves de cifrado predeterminadas se hayan cambiado al momento de la instalación y que se cambien cada vez que una persona con conocimiento de éstas cese en sus funciones o se traslade a otro cargo en la empresa			
	2.1.1.b Verifique que se hayan cambiado las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos.			
	2.1.1.c Verifique que se hayan cambiado las contraseñas predeterminadas de los puntos de acceso.			
	2.1.1.d Verifique que el firmware de los dispositivos inalámbricos esté actualizado a los efectos de admitir el cifrado sólido para la autenticación y transmisión en redes inalámbricas.			
	2.1.1.e Verifique que se hayan cambiado otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda.			

Requisitos de las PCI DSS	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. Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo: ▪ Center for Internet Security (CIS) ▪ International Organization for Standardization (ISO) ▪ SysAdmin Audit Network Security (SANS) Institute ▪ National Institute of Standards Technology (NIST)	**2.2.a** Examine las normas de configuración de sistemas de la organización correspondientes a todos los tipos de componentes de sistemas y verifique que las normas de configuración de sistemas concuerden con las normas de alta seguridad aceptadas en la industria.			
	2.2.b Verifique que las normas de configuración de sistemas se actualicen a medida que se identifiquen nuevas vulnerabilidades, tal como se define en el Requisito 6.2.			
	2.2.c Verifique que las normas de configuración de sistemas se apliquen al configurar nuevos sistemas.			
	2.2.d Verifique que las normas de configuración de sistemas incluyan cada punto que aparece a continuación (2.2.1 – 2.2.4).			
2.2.1 Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor. (Por ejemplo, los servidores web, servidores de base de datos y DNS se deben implementar en servidores separados). ***Nota:*** *Cuando se utilicen tecnologías de virtualización, implemente sólo una función principal por componente de sistema virtual.*	**2.2.1.a** En el caso de la muestra de componentes del sistema, verifique que sólo una función principal se haya implementado en cada servidor.			
	2.2.1.b Si se utilizan tecnologías de virtualización, verifique que sólo se haya implementado una función principal por componente de sistema o dispositivo virtual.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
2.2.2 Habilite sólo los servicios, protocolos, daemons, etc. necesarios y seguros, según lo requiera la función del sistema. Implemente funciones de seguridad para todos los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSec VPN, para proteger servicios no seguros, tales como NetBIOS, archivos compartidos, Telnet, FTP, etc.	**2.2.2.a** En el caso de la muestra de componentes de sistema, inspeccione los servicios, daemons y protocolos habilitados del sistema. Verifique que sólo se habiliten los servicios o protocolos necesarios.			
	2.2.2.b Identifique todos los servicios, daemons o protocolos habilitados. Verifique que se hayan justificado y que las funciones de seguridad se hayan documentado e implementado.			
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 verificar que conocen las configuraciones comunes de parámetros de seguridad para los componentes de sistemas.			
	2.2.3.b Verifique 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, verifique que los parámetros de seguridad comunes se hayan configurado adecuadamente.			
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.a** En el caso de la muestra de componentes del sistema, verifique que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos, etc.) .			
	2.2.4.b. Verifique que las funciones habilitadas se documenten y respalden una configuración segura.			
	2.2.4.c. Verifique que sólo la funcionalidad documentada esté presente en la muestra de componentes del sistema.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y el acceso administrativo que no sea de consola.	**2.3** En el caso de la muestra de componentes del sistema, verifique que el acceso administrativo que no sea de consola se cifre mediante:			
	2.3.a Observe a 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.			
	2.3.b Revise los servicios y archivos de parámetros en los sistemas a fin de determinar que Telnet y otros comandos de conexión remota no están disponibles para uso interno.			
	2.3.c Verifique 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 hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el *Anexo A: Requisitos adicionales de las PCI DSS para los proveedores de servicios de hosting compartido.*	**2.4** Realice los procedimientos de prueba desde **A.1.1** hasta **A.1.4** que se describen en *Anexo A: Requisitos adicionales de las PCI DSS para los proveedores de servicios de hosting* en lo que respecta a la evaluación de las PCI DSS de los proveedores de hosting compartido para verificar que estos proveedores protejan los datos y el entorno sujeto al hosting de las entidades (comerciantes y proveedores de servicios).			

Proteger 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 y obtiene acceso a los datos cifrados, sin las claves de cifrado 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 titulares de tarjetas salvo que sea absolutamente necesario, truncar los datos de titulares de tarjetas si no se necesita el PAN completo y no enviar el PAN utilizando tecnologías de mensajería de usuario final, tales como correos electrónicos y mensajería instantánea.

Consulte el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS* para obtener definiciones de "cifrado sólido" y otros términos de las PCI DSS.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos, como se indica abajo.	**3.1** Obtenga y examine las políticas, los procedimientos y los procesos relativos a la retención y disposición de datos y haga lo siguiente:			
3.1.1 Implemente una política de retención y disposición de datos que incluya: ▪ Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio ▪ Procesos para eliminar datos de manera cuando ya no se necesiten ▪ Requisitos de retención específicos para datos de titulares de tarjetas	**3.1.1.a** Verifique que las políticas y los procedimientos se implementen y que incluyan los requisitos legales, reglamentarios y del negocio relativos a la retención de los datos, incluidos los requisitos específicos para la retención de datos de titulares de tarjetas (por ejemplo, es necesario guardar los datos de titulares de tarjetas durante X tiempo por Y razones de negocio).			
	3.1.1.b Verifique que las políticas y los procedimientos incluyan cláusulas para la disposición de los datos cuando ya no sean necesarios por razones legales, reglamentarias o del negocio, incluida la disposición de datos de titulares de tarjetas.			
	3.1.1.c Verifique que las políticas y los procedimientos incluyan todo el almacenamiento de datos de titulares de tarjetas.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
▪ Un proceso automático o manual trimestral para identificar y eliminar de manera segura los datos de titulares de tarjetas almacenados que excedan los requisitos de retención definidos	**3.1.1.d** Verifique que las políticas y los procedimientos incluyan por lo menos una de las siguientes: Un proceso programático (automático o manual) para eliminar, por lo menos trimestral, datos de titulares de tarjetas almacenados que excedan los requisitos definidos en la política de retención de datos Requisitos para una revisión, la cual se debe realizar por lo menos trimestralmente, para verificar que los datos de titulares de tarjetas almacenados no excedan los requisitos definidos en la política de retención de datos.			
	3.1.1.e En el caso de una muestra de componentes del sistema que almacenan datos de titulares de tarjetas, verifique que los datos almacenados no excedan los requisitos definidos en la política de retención de datos.			
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: ***Nota:*** *Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos confidenciales de autenticación si existe una justificación de negocio y los datos se almacenan de forma segura.*	**3.2.a** En el caso de los emisores de tarjetas y/o las empresas que respaldan servicios de emisión y almacenan datos confidenciales de autenticación, verifique que exista una justificación de negocio para el almacenamiento de datos confidenciales de autenticación y que dichos datos están asegurados.			
	3.2.b En el caso de otras entidades, si se reciben y eliminan datos de autenticación confidenciales, obtenga y revise los procesos de eliminación segura de datos a fin de verificar que los datos son irrecuperables.			
	3.2.c Por cada tipo de dato de autenticación confidencial que aparece a continuación, realice los siguientes pasos:			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.2.1 No almacene contenido completo de ninguna pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo). Estos datos se denominan alternativamente pista completa, pista, pista 1, pista 2 y datos de banda magnética. ***Nota:*** *En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:* ▪ *El nombre del titular de la 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.*	**3.2.1** En el caso de la muestra de componentes del sistema, examine las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que el contenido completo de cualquier pista de la banda magnética en el reverso de la tarjeta o cualesquiera datos almacenados en un chip no se almacenen bajo 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			
3.2.2 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.	**3.2.2** En el caso de la muestra de componentes del sistema, examine las fuentes de datos y verifique, incluyendo, pero sin limitarse a, 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 bajo 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 las fuentes de datos y evalúe, incluyendo, pero sin limitarse a, que los PIN y los bloqueos de PIN cifrados no se			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
	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.**3.3**			
3.4 Haga que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos: ▪ Valores hash de una vía basados en criptografía sólida (el hash debe ser de todo el PAN). ▪ Truncamiento (los valores hash no	**3.4.aObtenga 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). Verifique que el PAN quede ilegible mediante el uso de uno de los siguientes métodos:** ▪ Valores hash de una vía en criptografía sólida ▪ Truncamiento. ▪ Token y ensambladores de índices (los ensambladores se deben almacenar de manera segura). ▪ Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
se pueden usar para reemplazar el segmento truncado del PAN) ▪ Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). ▪ Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas. ***Nota:*** *Para una persona maliciosa sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncada del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncada no se puedan correlacionar para reconstruir el PAN original.*	**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 copias de seguridad en cintas) para confirmar que el PAN sea ilegible.			
	3.4.d Examine una muestra de los archivos de auditoría para confirmar que el PAN queda ilegible o es eliminado 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 Verifique que las claves criptográficas estén almacenadas de forma segura (por ejemplo, se almacenen en medios portátiles protegidos adecuadamente con controles sólidos de acceso).			
	3.4.1.c Verifique que los datos de los titulares de las tarjetas almacenados en medios portátiles se cifren donde quiera que se almacenen. ***Nota:*** *Si no se utiliza el cifrado de disco para cifrar medios portátiles, los datos almacenados en estos medios deberán quedar ilegibles mediante algún otro método.*			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.5 Proteja las claves utilizadas para asegurar los datos de los titulares de tarjeta contra divulgación o uso indebido. ***Nota:*** *Este requisito también se aplica a las claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos; tales claves de cifrado de claves deben ser por lo menos tan sólidas como la clave de cifrado de datos*.	**3.5** Verifique 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.a** Examine los archivos de configuración del sistema para verificar que las claves se almacenan en formato cifrado y que las claves de cifrado de claves se almacenan separadas de la claves de cifrado de datos.			
	3.5.2.b Identifique las ubicaciones de almacenamiento de claves para verificar que las claves estén almacenadas en la menor cantidad de ubicaciones y formas posibles.			
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: ***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.a** Verifique la existencia de procedimientos de gestión de claves de las claves que se utilizan para el cifrado de datos de titulares de tarjetas.			
	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, de conformidad con los requisitos 3.6.1 a 3.6.8 que aparecen a continuación.			
	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** Verifique que los procedimientos de gestión de claves se hayan implementado para requerir la generación de claves sólidas.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.6.2 Distribución segura de claves criptográficas	**3.6.2** Verifique que los procedimientos de administración de claves se hayan implementado para solicitar la distribución de claves seguras.			
3.6.3 Almacenamiento seguro de claves criptográficas	**3.6.3** Verifique que los procedimientos de administración de clave se hayan implementado para solicitar el almacenamiento de claves seguras.			
3.6.4 La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria (por ejemplo, NIST Special Publication 800-57).	**2.6.4** Verifique que los procedimientos de gestión de claves se hayan implementado para requerir los cambios de clave al final del período de cifrado definido.			
3.6.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción y/o revocación) según se considere necesario cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro, etc.) o cuando se sospeche que las claves están en riesgo. ***Nota:*** *Si es necesario retener las claves criptográficas retiradas o reemplazadas, éstas se deben archivar de forma segura (por ejemplo, utilizando una clave de cifrado de claves). Las claves criptográficas archivadas se deben utilizar sólo con fines de descrifrado/verificación.*	**3.6.5.a** Verifique que los procedimientos de gestión de claves se hayan implementado para retirar las claves cuando se haya debilitado la integridad de las mismas.			
	3.6.5.b Verifique que los procedimientos de gestión de claves se hayan implementado para solicitar el reemplazo de claves que se sepa o se sospeche estén en riesgo.			
	3.6.5.c Si se retienen las claves criptográficas retiradas o reemplazadas, verifique que la aplicación no las utilice para operaciones de cifrado.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
3.6.6 Si se utilizan operaciones manuales de gestión de claves criptográficas en texto claro, estas operaciones deben aplicar conocimiento dividido y control doble (por ejemplo, utilizando dos o tres personas, cada una de las cuales conoce su propia parte de la clave, para reconstruir toda la clave). ***Nota:*** *Los ejemplos de operaciones manuales de gestión de claves incluyen, entre otros: generación, transmisión, carga, almacenamiento y destrucción de claves.*	**3.6.6** Verifique que los procedimientos manuales de gestión de claves en texto claro requieran conocimiento dividido y control doble de las claves.			
3.6.7 Prevención de sustitución no autorizada de claves criptográficas.	**3.6.7** Verifique que los procedimientos de gestión de claves se hayan implementado para solicitar la prevención de sustitución no autorizada de claves.			
3.6.8 Requisito de que los custodios de claves criptográficas declaren formalmente que comprenden y aceptan su responsabilidad como custodios de las claves.	**3.6.8** Verifique que los procedimientos de administración de clave se hayan implementado para solicitar que los custodios de claves declaren (por escrito o electrónicamente) que comprenden y acepten sus responsabilidades como custodios de claves.			

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las 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 siguen siendo 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 PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
4.1 Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas. *Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las PCI DSS incluyen, pero sin limitarse a:* ▪ The Internet ▪ Tecnologías inalámbricas ▪ Sistema global para comunicaciones móviles (GSM) ▪ Servicio de radio paquete general (GPRS)	**4.1** Verifique el uso de protocolos de seguridad siempre que se transmitan o reciban datos de los titulares de las tarjetas a través de redes públicas abiertas. Verifique que se use el cifrado sólido durante la transmisión de datos, de la siguiente manera:			
	4.1.a Seleccione una muestra de transacciones a medida que se reciben y observe las transacciones que se llevan a cabo para verificar que los datos de los titulares de las tarjetas se cifran durante el tránsito.			
	4.1.b Verifique que sólo se acepten claves/certificados SSL/TSL de confianza.			
	4.1.c Verifique que se haya implementado el protocolo para utilizar sólo configuraciones de seguridad, y que no se admitan versiones o configuraciones inseguras.			
	4.1.d Verifique que se implemente la solidez de cifrado adecuada para la metodología que se utiliza. (Consulte las recomendaciones/mejores prácticas de los proveedores).			
	4.1.e Para implementaciones de SSL/TLS: ▪ 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.			

Requisitos de las PCI DSS	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. ***Nota:*** *La utilización de WEP como control de seguridad se prohibió a partir 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, el chat, etc.).	**4.2.a** Verifique que el PAN quede ilegible o asegurado con cifrado sólido cada vez que se envíe mediante tecnologías de mensajería de usuario final.			
	4.2.b Verifique 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.			

Mantener 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 de negocio 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 PCI DSS	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, verifique 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 estos.	**5.1.1** En el caso de la muestra de componentes del sistema, verifique 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 estén actualizados, estén en funcionamiento y puedan generar registros de auditoría.	**5.2** Verifique 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 examine la política y controle que solicite la actualización del software antivirus y las definiciones.			
	5.2.b Verifique 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.			
	5.2.d En el caso de la muestra de componentes del sistema, verifique que la generación de registro de software antivirus esté habilitada y que esos registros se almacenen conforme al Requisito 10.7 de las PCI DSS.			

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 PCI DSS	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 para protección contra vulnerabilidades conocidas. 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 Examine 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente. ***Notas:*** ▪ *Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria. Por ejemplo, los criterios para clasificar vulnerabilidades de "Alto" riesgo pueden incluir una puntuación base CVSS de 4.0 o superior, y/o un parche proporcionado por el proveedor clasificado por el mismo como "crítico", y/o una vulnerabilidad que afecte un componente crítico del sistema.* ▪ *La clasificación de vulnerabilidades según lo definido en 6.2.a es considerada una buena práctica hasta el 30 de junio de 2012, y a partir de entonces se convierte en un requisito.*	**6.2.a** Consulte al personal responsable para verificar que se implementan procesos para identificar nuevas vulnerabilidades de seguridad, y que se haya asignado una clasificación de riesgo a esas vulnerabilidades. (Como mínimo, las vulnerabilidades más críticas que representen los riesgos más altos se deben clasificar como "Alto".			
	6.2.b Verifique que los procesos para identificar las nuevas vulnerabilidades de seguridad incluyan el uso de fuentes externas de información sobre vulnerabilidades de seguridad.			
6.3 Desarrolle aplicaciones de software (acceso interno y externo, e incluso acceso administrativo basado en la web a aplicaciones) de conformidad con las PCI DSS (por ejemplo, autenticación segura y registro), basadas en las mejores prácticas de la industria. Incorpore seguridad de la información en todo el ciclo de vida de desarrollo del software. Estos procesos deben incluir lo siguiente:	**6.3.a** Obtenga y examine los procesos de desarrollo de software escritos para verificar que los procesos estén basados en normas de la industria y/o en las mejores prácticas.			
	6.3.b Examine que se incluya la seguridad de la información en todo los procesos de desarrollo de software escritos.			
	6.3.c Examine los procesos de desarrollo de software escritos para verificar que esas aplicaciones de software se desarrollen en conformidad con las PCI DSS.			
	6.3.d Utilizando un examen de los procesos de desarrollo de software escritos y entrevistas a los desarrolladores de software, verifique que:			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.3.1 Eliminación de las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes de que las aplicaciones se activen o se pongan a disposición de los clientes	**6.3.1** Las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación se eliminan antes de activar los sistemas de producción o de que se pongan a disposición de los clientes.			
6.3.2 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.* *Las revisiones de los códigos pueden ser realizadas por terceros o por 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 PCI DSS.*	**6.3.2.a** Obtenga y analice las políticas para confirmar que todos los cambios a los códigos de aplicaciones personalizadas de se deban revisar (ya sea mediante procesos manuales o automáticos) de la siguiente manera: ▪ Los cambios a los códigos son revisados por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura. ▪ Las revisiones de los códigos aseguran que estos se desarrollan de acuerdo con las directrices de codificación segura (consulte el requisito 6.5 de las PCI DSS). ▪ Las correcciones pertinentes se implementan antes del lanzamiento. ▪ La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento.			
	6.3.2.b Seleccione una muestra de cambios recientes de aplicaciones personalizadas y controle que los códigos de aplicaciones personalizadas se revisen conforme a 6.3.2.a que aparecen anteriormente.			
6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Los procesos deben incluir lo siguiente:	**6.4** A partir de un examen de procesos de control de cambios, entrevistas con administradores de sistemas y redes, y un examen de datos relevantes (documentación de configuración de redes, datos y producción y prueba, etc.), verifique lo siguiente:			
6.4.1 Desarrollo/prueba por separado y entornos de producción	**6.4.1** Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control del acceso para reforzar la separación.			
6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción	**6.4.2** Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo	**6.4.3** Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo.			
6.4.4 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción	**6.4.4** Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción.			
6.4.5 Procedimientos de control de cambios para la implementación de parches de seguridad y modificaciones del software. Los procedimientos deben incluir lo siguiente:	**6.4.5.a** Verifique que los procedimientos de control de cambio relacionados con la implementación de los parches de seguridad y las modificaciones de software estén documentados y que los procedimientos incluyan los puntos 6.4.5.1 – 6.4.5.4 que aparecen a continuación.			
	6.4.5.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 examine, realice lo siguiente:			
6.4.5.1 Documentación de incidencia.	**6.4.5.1** Verifique que la documentación que tiene incidencia se incluya en la documentación de control de cambios de cada cambio.			
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.	**6.4.5.2** Verifique que la aprobación documentada por partes autorizadas esté presente para cada muestra de cambio.			
6.4.5.3 Verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.	**6.4.5.3.a** Para cada cambio probado, verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.			
	6.4.5.3.b En el caso de cambios del código personalizado, verifique que se hayan realizado las pruebas a todas las actualizaciones de conformidad con el requisito 6.5 de las PCI DSS antes de la implementación para producción.			
6.4.5.4 Procedimientos de desinstalación.	**6.4.5.4** Verifique que se prepare los procedimientos de desinstalación para cada cambio.			
6.5 Desarrolle aplicaciones basadas en directrices de codificación seguras. Evite vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir: ***Nota:*** *Las vulnerabilidades que se*	**6.5.a** Obtenga y revise los procesos de desarrollo de software. Verifique que el proceso requiera capacitación acerca de las técnicas de codificación segura para desarrolladores, que esté basada en las mejores prácticas de la industria, así como asesoría.			
	6.5.b Entreviste a un grupo modelo de desarrolladores y obtenga pruebas de que son expertos en técnicas de codificación segura.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
enumeran desde el punto 6.5.1 hasta el 6.5.9 eran congruentes con las mejores prácticas de la industria cuando se publicó esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.	**6.5.c.** Verifique que existan procesos implementados para garantizar que las aplicaciones no son vulnerables, como mínimo, a lo siguiente:			
6.5.1 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.	**6.5.1** Errores de inyección, en especial, errores de inyección SQL. (valide la entrada para verificar que los datos de usuario no pueden modificar el significado de los comandos y las consultas, utilice las consultas basadas en parámetros, etc.).			
6.5.2 Desbordamiento de buffer	**6.5.2** Desbordamiento de buffer (validar límites del buffer y truncar cadenas de entrada).			
6.5.3 Almacenamiento cifrado inseguro	**6.5.3** Almacenamiento cifrado inseguro (prevenir defectos de cifrado).			
6.5.4 Comunicaciones inseguras	**6.5.4** Comunicaciones inseguras (cifrar adecuadamente todas las comunicaciones autenticadas y confidenciales).			
6.5.5 Manejo inadecuado de errores	**6.5.5** Manejo inadecuado de errores (no permitir que se filtre información a través de mensajes de error)			
6.5.6 Todas las vulnerabilidades “altas” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.2 de las PCI DSS). ***Nota:*** *Este requisito se considera una mejor práctica hasta el 30 de junio de 2012, y a partir de entonces se convierte en requisito.*	**6.5.6** Todas las vulnerabilidades “altas” identificadas en el Requisito 6.2 de las PCI DSS.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
Nota: *Los requisitos del 6.5.7 al 6.5.9, que siguen, se aplican a las aplicaciones basadas en la web y a las interfaces de aplicaciones (internas o externas):*				
6.5.7 Lenguaje de comandos entre distintos sitios (XSS)	**6.5.7** Lenguaje de comandos entre distinto sitios (XSS) (valide todos los parámetros antes de la inclusión, utilice técnicas de escape sensibles al contexto, etc.).			
6.5.8 Control de acceso inapropiado (tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios)	**6.5.8** Control de acceso inapropiado tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios (Autentique usuarios de forma correcta y desinfecte entradas. No exponga referencias a objetos internos a usuarios).			
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF)	**6.5.9** Falsificación de solicitudes entre distintos sitios (CSRF). (No confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente).			

Requisitos de las PCI DSS	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:*** *"Una organización que se especialice en seguridad de aplicaciones" 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.*			

Implementar medidas sólidas de control de acceso

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.

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

Requisitos de las PCI DSS	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 examine la política escrita sobre control de datos y verifique 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** Confirme 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** Confirme 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 roles” o RBAC).			
7.1.3 Requisito de una aprobación documentada de partes autorizadas especificando privilegios requeridos.	**7.1.3** Confirme que se requiera aprobación documentada de partes autorizadas (por escrito o electrónicamente) para todo el acceso, y que se deben especificar los privilegios requeridos.			
7.1.4 Implementación de un sistema de control de acceso automático	**7.1.4** Confirme que los controles de acceso se implementen a través de un sistema de control de acceso automático.			
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 que se configure para “negar todo”, salvo que se permita específicamente. 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:			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
7.2.1 Cobertura de todos los componentes del sistema	**7.2.1** Confirme 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** Confirme 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" ***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.*	**7.2.3** Confirme que los sistemas de control de acceso posean un ajuste predeterminado de "negar todos".			

Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora

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.

Nota: *Estos requisitos se aplican a todas las cuentas, incluidas las cuentas de puntos de venta, con capacidades administrativas y todas las cuentas utilizadas para ver o acceder a datos de titulares de tarjetas o para acceder a sistemas con datos de titulares de tarjetas. Sin embargo, los Requisitos 8.1, 8.2 y 8.5.8 al 8.5.15 no se aplican a las cuentas de usuarios dentro de una aplicación de pago de un punto de venta que sólo tengan acceso a un número de tarjeta por vez a fin de facilitar una transacción única (tales como las cuentas en efectivo).*

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 o 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 todos los usuarios: ▪ Algo que el usuario sepa, como una contraseña o frase de seguridad ▪ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente ▪ Algo que el usuario sea, como un rasgo biométrico	**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 examine 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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. (Por ejemplo, autenticación remota y servicio dial-in (RADIUS) con tokens; sistema de control de acceso mediante control del acceso desde terminales (TACACS) con tokens; u otras tecnologías que faciliten la autenticación de dos factores). ***Nota:*** *La autenticación de dos factores requiere que se utilicen dos de los tres métodos de autenticación (consulte el Requisito 8.2 para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de dos factores.*	**8.3** Para verificar que la autenticación de dos factores está implementada para todo acceso remoto a la red, observe a un empleado (por ejemplo, un administrador) mientras se conecta a la red de manera remota y verifique se utilizan dos de los tres métodos de autenticación.			
8.4 Deje ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante un cifrado sólido.	**8.4.a** En el caso de la 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 servicios, 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	**8.5.1** 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			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
otros objetos de identificación.	política mediante las siguientes acciones: ▪ Obtenga y examine un formulario de autorización de cada ID. ▪ Verifique que las ID de usuario 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/autenticación 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, y las contraseñas restablecidas para usuarios existentes, se configuren en un valor único para cada usuario y se cambien después del primer uso.			
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/inhabilite las cuentas de usuario inactivas al menos cada 90 días.	**8.5.5** Verifique que se eliminen o se inhabiliten las cuentas que lleven más de 90 días inactivas.			
8.5.6 Habilite las cuentas que utilicen los proveedores para el acceso remoto únicamente durante el período necesario. Supervise las cuentas de acceso remoto de proveedores cuando se utilicen.	**8.5.6.a** Verifique que cualquiera de las cuentas utilizadas por los proveedores para acceder, respaldar y mantener los componentes del sistema estén inhabilitadas, y que el proveedor las habilite sólo cuando sea necesario.			
	8.5.6.b Verifique que se supervisen las cuentas de acceso remoto de los proveedores mientras se utilizan.			
8.5.7 Comunique los procedimientos y las políticas de autenticación a todos los usuarios con 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 las políticas de autenticación.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.8 No utilice cuentas ni contraseñas de grupos, compartidas o genéricas, ni ningún otro método de autenticación.	**8.5.8.a** En el caso de la muestra de componentes del sistema, examine las listas de ID de usuario y verifique lo siguiente: ▪ Las ID de usuario y cuentas genéricas se encuentran inhabilitadas 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 para verificar que están explícitamente prohíbidas las contraseñas de grupo y compartidas y otros métodos de autenticación.			
	8.5.8.c Entreviste a los administradores del sistema para verificar que las contraseñas de grupo y compartidas y otros métodos de autenticación no se distribuyan, aunque sean solicitadas.			
8.5.9 Cambie las contraseñas de usuario al menos cada 90 días.	**8.5.9.a** En el case de la 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.			
	8.5.9.a Para proveedores de servicio únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite periódicamente que el cliente no consumidor 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.	"**8.5.10A 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."**			
	8.5.10.b 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 no consumidor cumplan con un requisito mínimo de cantidad de caracteres.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
8.5.11 Utilice contraseñas que contengan tanto caracteres numéricos como alfabéticos.	**8.5.11.a** 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 se encuentren configurados de manera que se solicite que incluyan caracteres numéricos y alfabéticos.			
	8.5.11.b 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 no consumidor incluyan tanto caracteres numéricos como alfabéticos.			
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** En en el caso de la muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que se solicite que las nuevas contraseñas no sean iguales a las últimas cuatro contraseñas utilizadas anteriormente.			
	8.5.12.b Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que las nuevas contraseñas de cliente no consumidor 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** En el caso de la muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de autenticación 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.			
	8.5.13.b Para proveedores de servicios únicamente, revise los procesos internos y la documentación del cliente/usuario para verificar que las cuentas de usuarios no 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** En el caso de la muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del 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			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
	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** En el caso de la 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.			
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. Restrinja el acceso directo a o las consultas en las bases de datos a los administradores de la base de datos.	**8.5.16.a** Revise los valores de confirguración de la base de datos y las aplicaciones y verifique que todos los uusarios se haya autenticado antes del acceso.			
	8.5.16.b Verifique que los valores de configuración garanticen que 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).			
	8.5.16.c Verifique que los parámetros de configuración de bases de datos y aplicaciones limiten el acceso directo y las consultas a las bases de datos a los administradores de bases de datos.			
	8.5.16.d 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: Restringir el acceso físico a los datos del titular de la tarjeta

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. A los fines del Requisito 9, “empleados” se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que estén físicamente presentes 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 durante un tiempo no prolongado, generalmente no más de un día. “Medios” se refiere a todos los medios en papel y electrónicos que contienen datos de titulares de tarjetas.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico 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 y 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.a** Verifique que las cámaras de video y/o otros mecanismos de control de acceso estén funcionando correctamente para supervisar los puntos de entrada/salida de áreas confidenciales.			
	9.1.1.b Verifique que las cámaras de video y/o otros mecanismos de control de acceso estén protegidos contra contra alteraciones y desactivaciones.			
	9.1.1.c Verifique que las cámaras de video y/o otros mecanismos sean supervisados y los datos de dichas cámaras o mecanismos se almacenen durante al menos tres meses.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.1.2 Restrinja el acceso físico a conexiones de red de acceso público. Por ejemplo, las áreas que sean accesibles a los visitantes no deben tener puertos de red habilitados a menos que se autorice explícitamente el acceso a la red.	**9.1.2Verifique que sólo empleados autorizados habiliten las conexiones de red en sitio sólo cuando sea necesario realizando entrevistas y observando. De forma alternativa, verifique que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.**			
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones.	**9.1.3** Verifique que el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones haya sido correctamente limitado.			
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.	**9.2.aRevise 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:** ▪ Asignación de placas de identificación, ▪ Cambio de requisitos de acceso y ▪ Revocación de placas de identificación de personal local cesante y de visitante vencidas			
	9.2.b Verifique que el acceso al sistema de placas de identificación esté limitado al personal autorizado.			
	9.2.c Examine las placas de identificación que se estén utilizando para verificar que identifiquen claramente a los visitantes y que sean fáciles de distinguir respecto a las placas del personal local.			
9.3 Asegúrese de que todos los visitantes reciban el siguiente trato:	**9.3**Verifique que los controles realizados a 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** Observe el uso de las placas de identificación de visitantes para verificar que una placa de identificación de visitante no permita el acceso sin escolta a las áreas en las que se almacenan físicamente datos de los 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.a** Observe a las personas dentro de las instalaciones de la empresa para verificar el uso de placas de identificación de visitantes y que los visitantes se puedan distinguir fácilmente del personal que trabaja en la empresa.			
	9.3.2.b Verifique que las placas de identificación del personal tengan vencimiento.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
9.3.3 Confirme que le sea solicitado entregar el 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 mantener 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.bVerifique 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.a** Observe la seguridad física de la localidad de almacenamiento para confirmar que el almacenamiento del medio de la copia de seguridad esté protegido.			
	9.5.b Verifique que la seguridad de la localidad de almacenamiento sea revisada por lo menos anualmente.			
9.6 Proteja físicamente todos los medios.	**9.6** Verifique que los procedimientos para proteger los datos de titulares de tarjetas incluyan controles para el resguardo seguro de todos los medios (incluidos pero no limitados a: computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faxes).			
9.7Lleve 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 pueda determinar la confidencialidad de los datos.	**9.7.1** Verifique que todos los medios se hayan clasificado de manera que la sensibilidad de los datos se pueda determinar.			
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 reciente 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.	**9.9**Obtenga y examine la política para controlar el almacenamiento y mantenimiento de todos los medios 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 el negocio 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).			

Supervisar y evaluar las redes con regularidad

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las 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, casi imposible, 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, examen de los registros de auditoría, examen de la configuración del registro 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 se registren 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 de la aplicación	**10.2.6**Verifique que esté registrada la inicialización de los registros de auditoría.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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 incluya en las entradas del registro.			
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	**10.3.3** Verifique que el sello de fecha y hora se incluya en las entradas del registro.			
10.3.4 Indicación de éxito o fallo	**10.3.4Verifique que la indicación de éxito u omisión se incluya en las entradas del registro.**			
10.3.5 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 Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos. ***Nota:*** *Un ejemplo de tecnología de sincronización es el Protocolo de tiempo de la red (Network Time Protocol (NTP).*	**10.4.a** Verifique que la tecnología de sincronización se implemente y mantenga actualizada, según los Requisitos de las PCI DSS 6.1 y 6.2.			
	10.4.b 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:			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
10.4.1 Los sistemas críticos tienen horario uniforme y correcto.	**10.4.1.a** Verifique que sólo los servidores de horario centrales designados reciban señales de tiempo de las fuentes externas y que las señales de tiempo externas estén basadas en la hora atómica internacional o UTC.			
	10.4.1.b Verifique que los servidores de tiempo central designados interactúen entre sí para mantener un tiempo exacto y que otros servidores internos reciban señales de tiempo sólo de los servidores de tiempo centrales.			
10.4.2 Los datos de tiempo están protegidos.	**10.4.2.a** Revise las configuraciones del sistema y los valores de configuración de sincronización para verificar que el acceso a los datos de tiempo esté limitado sólo a personal que tenga necesidad de negocios de tener acceso a los datos de tiempo.			
	10.4.2.b Revise las configuraciones del sistema y tanto los valores de configuración como los procesos de sincronización para verificar que cualquier cambio de configuración de tiempo en los sistemas críticos sea registrado, supervisado y revisado.			
10.4.3 La configuración de tiempo se recibe de fuentes aceptadas por la industria.	**10.4.3** Verifique que los servidores de tiempo acepten actualizaciones de tiempo de fuentes externas específicas, aceptadas por la industria (para evitar que individuos con intenciones fraudulentas cambien 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 a los que se proporcionarán las actualizaciones de tiempo (para evitar el uso no autorizado de servidores de hora internos).			
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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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 que interactúen con la parte externa en un servidor de registros en la LAN interna.	**10.5.4**Verifique que registros para tecnologías que interactúan con la parte externa (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 supervisión 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 supervisión de integridad de archivos o de detección de cambios para registros mediante el análisis de los parámetros del sistema, de los archivos supervisados y de los resultados de dicha supervisión.			
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	**10.7.a**Obtenga y examine las políticas y los 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).	**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 Realice pruebas para detectar la presencia de puntos de acceso inalámbrico y de puntos de acceso inalámbrico no autorizados trimestralmente. ***Nota:*** *Los métodos que se pueden utilizar en este proceso incluyen, sin limitarse a estos, barridos de redes inalámbricas, inspecciones lógicas/físicas de componentes y de la infraestructura de sistemas, control de acceso a la red (NAC) o IDS/IPS inalámbrico.* *El o los métodos que se utilicen deben ser capaces de detectar e identificar cualquier dispositivo no autorizado.*	**11.1.a** Verifique que la entidad tenga un proceso documentado para detectar e identificar puntos de acceso inalámrico trimestralmente.			
	11.1.b Verifique que la metodología sea la adecuada para detectar e identificar cualquier punto de acceso, incluyendo por lo menos lo siguiente: ▪ tarjetas WLAN insertadas en los componentes del sistema ▪ Dispositivos inalámbricos conectados a componentes del sistema (por ejemplo, por USB, etc.) ▪ Dispositivos inalámbricos conectados a un puerto de red o a un dispositivo de red			
	11.1.c Verifique que el proceso documentado para identificar los puntos de acceso inalámbricos no autorizados sea realizado por lo menos trimestralmente para todos los componentes e instalaciones de sistemas.			
	11.1.d Si se utiliza supervisión automatizada (por ejemplo, IDS/IPS inalámbrico, NAC, etc.), verifique que la configuración generará alertas al personal.			
	11.1.e 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:*** *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. En el caso de los años siguientes a la revisión inicial de las PCI DSS, deben obtenerse cuatro análisis aprobados.*	**11.2** Verifique que se realicen análisis de vulnerabilidad externa e interna de la manera siguiente:			
11.2.1 Realice análisis de vulnerabilidad interna trimestralmente.	**11.2.1.a** Revise los informes de los análisis y verifique que se hayan realizado cuatro análisis internos trimestrales durante el período de 12 meses más reciente.			
	11.2.1.b Revise los informes de los análisis y verifique que el proceso de análisis incluya la repetición de los análisis hasta que se obtengan resultados de aprobación o hasta que se resuelvan todas las vulnerabilidades “Altas”, según la definición del Requisito 6.2 de las PCI DSS.			
	11.2.1.c 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).			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.2.2 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). ***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.*	**11.2.2.a** Revise los resultados de los cuatro trimestres más recientes de análisis de vulnerabilidad externa y verifique que se hayan realizado los cuatro análisis correspondientes al período de 12 meses más reciente.			
	11.2.2.b Revise los resultados de cada análisis trimestral para asegurar que cumplan con los requisitos de la Guía del programa ASV (por ejemplo, no hay vulnerabilidades con calificación mayor que 4.0, según la CVSS y no hay fallas automáticas).			
	11.2.2.c Revise los informes de los análisis para verificar que hayan sido realizados por un Approved Scanning Vendor (ASV), certificado por las PCI SSC.			
11.2.3 Realice análisis internos y externos después de cualquier cambio significativo. ***Nota:*** *Los análisis que se realicen después de los cambios pueden ser ejecutados por personal interno.*	**11.2.3.a** Inspeccione la documentación del control de cambios y los informes de análisis para verificar que los componentes del sistemas que hayan sufrido cambios significativos hayan sido analizados.			
	11.2.3.b Revise los informes de los análisis y verifique que el proceso de análisis incluye la repetición de los análisis hasta que: ▪ Para análisis externos, no se hayan registrado vulnerabilidades con puntuaciones mayores que 4.0, según la CVSS. ▪ Para análisis internos, se haya obtenido un resultado de aprobación o todas las vulnerabilidades “Alta”, como las define el Requisito 6.2 de las PCI DSS, hayan sido resueltas.			
	11.2.1.c 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).			

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.			
	11.3.b 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	**11.3.2Verifique que la prueba de penetración incluya pruebas de penetración de la capa de aplicación. Las pruebas deben incluir, por lo menos, las vulnerabilidades que contiene el Requisito 6.5.**			
11.4 Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores, líneas base y firmas de detección y prevención de intrusiones.	**11.4**Verifique el uso de los sistemas de detección y/o prevención de intrusiones y que todo el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares esté supervisado.			
	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 supervisión 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 supervisión 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 supervisión 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.a**Verifique el uso de los productos para supervisión de integridad de archivos en el entorno de datos de titulares de tarjetas mediante la observación de la configuración del sistema y los archivos supervisados, así como también de la revisión de los resultados de las actividades de supervisión. Ejemplos de archivos que se deben supervisar: ▪ Ejecutables del sistema ▪ Ejecutables de aplicaciones ▪ Archivos de configuración y parámetros ▪ Archivos de almacenamiento central, históricos o archivados, de registro y auditoría			
	11.5.b Verifique que las herramientas estén configuradas para alertar al personal respecto a la modificación no autorizada de archivos críticos y para realizar comparaciones de archivos críticos por lo menos semanalmente.			

Mantener una política de seguridad de información

Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal..

Una política de seguridad sólida establece el grado de seguridad para toda la entidad e informa a los empleados lo que se espera de ellos. Todos los empleados deben estar al tanto de la sensibilidad de los datos y de su responsabilidad para protegerlos. A los fines del Requisito 12, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la entidad o que tengan acceso al entorno de datos de los titulares de tarjetas.

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 de negocios).			
12.1.1 Aborda todos los requisitos de las PCI DSS.	**12.1.1** Verifique que la política aborde todos los requisitos de las PCI DSS.			
12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos. (Ejemplos de metodologías de evaluación de riesgos incluyen, pero no están limitados a: OCTAVE, ISO 27005 y NIST SP 800-30.)	**12.1.2.a** Verifique que se documente un proceso anual de evaluación de riesgos que identifique las amenazas, vulnerabilidades produzca como resultado una evaluación formal de riesgos.			
	12.1.2.b Revise la documentación de evaluación de riesgo para verificar que el proceso de evaluación de riesgos se ejecute por lo menos una vez al año.			
12.1.3 Incluye 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 del negocio 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**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 y de Internet) para definir el uso adecuado de dichas tecnologías. 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 por las partes autorizadas	**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 La activación de las tecnologías de acceso remoto para proveedores y socios de negocios solo cuando es necesaria para proveedores y socios de negocios, con desactivación inmediata después del uso	**12.3.9** Verifique que las políticas de uso requieran la activación de tecnologías de acceso remoto para proveedores y socios de negocios sólo cuando éstos lo requieran, con desactivación automática después de la utilización.			
12.3.10 Para que el personal tenga 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, a menos que sea autorizado explícitamente para una necesidad de negocios definida..	**12.3.10.a** 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.			
	12.3.10.b Para el personal con la autorización correcta, verifique que las políticas de uso requieran que los datos de los titulares de tarjetas sean protegidos, de acuerdo con los Requisitos de las PCI DSS.			
12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	**12.4**Verifique que las políticas de seguridad de la información definan con claridad las responsabilidades de seguridad de la información de todo el personal.			
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 los 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 procedimientos de respuesta ante incidentes de seguridad y escalación 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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.	**12.5.3**Verifique que la responsabilidad de crear y distribuir procedimientos de respuesta ante incidentes de seguridad y escalación haya sido formalmente asignada.			
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 todos los accesos a los datos esté formalmente asignada.			
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 al personal justo al ser contratado y, por lo menos, una vez al año. ***Nota:*** *Los métodos pueden cambiar, dependiendo del rol del empleado y de su nivel de acceso a los datos de los titulares de tarjetas.*	**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 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.7 Examine a los empleados antes de contratarlos a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias). ***Nota:*** *En el caso de empleados potenciales que serán contratados para ocupar ciertas posiciones, 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 potenciales 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.			
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 un reconocimiento 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.**			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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 mantenga un programa para supervisar el estado de cumplimiento con las 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:			
12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: ▪ Roles, 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.	**12.9.1a**Verifique que el plan de respuesta a incidentes incluya: ▪ Roles, 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.			
	12.9.1.b Revise la documentación de un incidente que se haya reportado o generado una alerta anteriormente para verificar que el plan y los procedimientos de respuesta se hayan seguido con el mencionado incidente.			
12.9.2Pruebe 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.			

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
12.9.3 Designe personal especializado que se encuentre disponible permanentemente (24/7) para responder a las alertas.	**12.9.3** Mediante la observación y revisión de las políticas, verifique que haya respuesta permanente (24/7) a incidentes y cobertura de supervisión 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 de sistema críticos o de contenido.			
12.9.4 Proporcione capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad.	**12.9.4Mediante 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 supervisión de integridad de archivos.	**12.9.5** Mediante observación y revisión de los procesos, verifique que el plan de respuestas a incidentes abarque la supervisión 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 las 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 las 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:			

Requisitos	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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.			
A.1.2 Limite el acceso y los privilegios de cada entidad sólo al entorno de datos de sus propios 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.dPara 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			

Requisitos	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
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** 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.			
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 las 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 las 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 todo 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 los usuarios individuales ejecuten comandos raíz sin que se los pueda rastrear o registrar.*

Anexo D: Segmentación y muestreo de instalaciones de negocios/Componentes de sistemas