PCI Security Standards Council

PCI (industria de tarjetas de pago)

Normas de seguridad de datos

Requisitos y procedimientos de evaluación de seguridad

Versión 3.2.1

Mayo de 2018

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción	Páginas
Octubre de 2008	1.2	Introducir la versión 1.2 de las PCI DSS (Normas de seguridad de datos de la industria de tarjetas de pago) como “requisitos de las PCI DSS y procedimientos de evaluación de seguridad” para eliminar la redundancia entre documentos e implementar cambios generales y específicos de los procedimientos de auditoría de seguridad de la versión 1.1 de las PCI DSS. Para obtener la información completa, consulte el Resumen de cambios de la Normas de seguridad de 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. Consulte *PCI DSS: Resumen de cambios de la versión 1.2.1 a 2.0 de las PCI DSS.*	
Noviembre de 2013	3.0	Actualización de la versión 2.0. Consulte *PCI DSS: Resumen de cambios de la versión 2.0 a 3.0 de las PCI DSS.*	
Abril de 2015	3.1	Actualización de la PCI DSS, versión 3.0. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.0 a 3.1*	
Abril de 2016	3.2	Actualización de la PCI DSS, versión 3.1. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.1 a 3.2*	
Mayo de 2018	3.2.1	Actualización de la PCI DSS, versión 3.2. Para obtener los detalles, consulte *PCI DSS – Resumen de cambios de la PCI DSS versión 3.2 a 3.2.1*.	

DECLARACIONES:

La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerarse, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

Índice

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

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas. La PCI DSS se aplica a ***todas*** las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a ***todas*** las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD). "A continuación, encontrará una descripción general de los 12 requisitos de las DSS de la PCI."

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

Desarrolle y mantenga redes y sistemas seguros.	**1.**	Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta.
	2.	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
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.**	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
	6.	Desarrollar y mantener sistemas y aplicaciones seguros
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.	Identificar y autenticar el acceso a los componentes del sistema.
	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 del titular de la tarjeta
	11.	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	**12.**	Mantener 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 pruebas comienzan en la página 15.

La PCI DSS comprende un conjunto mínimo de requisitos para proteger los datos de cuentas y se puede mejorar por medio de controles y prácticas adicionales a fin de mitigar los riesgos, así como leyes y regulaciones locales, regionales y sectoriales. Además, los requisitos de la legislación o las regulaciones pueden requerir la protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de tarjeta). Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales.

Recursos de las PCI DSS

El sitio web de *PCI Security Standards Council* (PCI SSC) (www.pcisecuritystandards.org) contiene algunos recursos adicionales para ayudar a las organizaciones con las evaluaciones y validaciones de las PCI DSS, entre otros:

- Biblioteca de documentos, que incluye lo siguiente:
  - *PCI DSS: Resumen de cambios de la versión 2.0 a 3.0 de las PCI DSS*
  - *Guía de referencia rápida de las PCI DSS*
  - *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS*
  - *Suplementos informativos y directrices*
  - *Enfoque priorizado para las PCI DSS*
  - *ROC (Informe sobre cumplimiento), plantilla para crear informes e instrucciones para crear informes*
  - *SAQ (Cuestionarios de autoevaluación) e instrucciones y directrices del SAQ*
  - *AOC (Atestación de cumplimiento)*
- Preguntas frecuentes (FAQ)
- PCI para los sitios web de pequeños comerciantes
- Cursos de capacitación y *webinars* informativos sobre PCI
- Lista de QSA (asesores de seguridad certificados) y ASV (proveedores aprobados de escaneo).
- Lista de dispositivos aprobados para la PTS (seguridad de la transacción con PIN) y aplicaciones de pagos validadas según las PA-DSS (Normas de seguridad de datos para las aplicaciones de pago)

***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 sustituyen, reemplazan ni extienden las PCI DSS ni ninguno de sus requisitos.*

Consulte *www.pcisecuritystandards.org* para obtener más información sobre estos y otros recursos.

Información sobre la aplicabilidad de las PCI DSS

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

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

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

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

Los requisitos de la PCI DSS se aplican a las organizaciones y entornos en los que se almacenan, procesan o transmiten datos de cuentas (datos del titular de la tarjeta y/o datos confidenciales de autenticación). Algunos requisitos de las PCI DSS también se aplican a organizaciones que han tercerizado las operaciones de pago o la gestión del CDE (entorno de los datos del titular de la tarjeta).[1] Además, las organizaciones que tercerizan el CDE (entorno de los datos del titular de la tarjeta) o las operaciones de pagos a terceros deben asegurarse de que estos protejan los datos de cuenta de acuerdo con todos los requisitos correspondientes de las PCI DSS.

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

[1] Según cada programa de cumplimiento de la marca de pago.

		Elemento de datos	Almacenamiento permitido	Datos almacenados ilegibles según el Requisito 3.4
Datos de cuentas	**Datos del titular de la tarjeta**	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN[5]	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.

No se deben almacenar los datos confidenciales de autenticación después de la autorización, incluso si están cifrados. Esto se implementa aún cuando no haya PAN en el entorno. Las organizaciones deben comunicarse con sus adquirientes o, directamente, con las marcas de pago para saber si pueden almacenar los SAD (datos de autenticación confidenciales) antes de la autorización, durante cuánto tiempo y para conocer cualquier requisito relacionado con la protección y el uso.

2 No se deben almacenar los datos de autenticación confidenciales después de la autorización (incluso si están cifrados).
3 Contenido completo de la pista que se encuentra en la banda magnética, datos equivalentes que se encuentran en el chip o en cualquier otro dispositivo
4 La cifra de tres o cuatro dígitos en el anverso o reverso de la tarjeta de pago
5 El número de identificación personal ingresado por el titular de la tarjeta durante una transacción con tarjeta presente o el bloqueo de PIN cifrado presente en el mensaje de la transacción.

Relación entre PCI DSS y PA-DSS

Aplicabilidad de las PCI DSS a las aplicaciones de las PA-DSS

El uso de una aplicación que cumpla con las PA-DSS por sí sola no implica que una entidad cumpla con las PCI DSS, 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.

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

Los requisitos de las PA-DSS se derivan de los *Requisitos de las PCI DSS y de los Procedimientos de evaluación de seguridad* (se definen en este documento). Las PA-DSS detallan los requisitos que debe cumplir una aplicación de pago a fin de facilitar el cumplimiento de las PCI DSS por parte del cliente. Como las amenazas de seguridad están en constante evolución, las aplicaciones que ya no reciben soporte del proveedor (por ejemplo, identificadas por el proveedor como "descontinuadas") pueden no ofrecer el mismo nivel de seguridad que las versiones que sí reciben soporte.

Cuando se implementen en un entorno que cumpla con las PCI DSS, las aplicaciones de pago seguro minimizarán tanto la posibilidad de fallos de seguridad que comprometan el PAN, el contenido completo de la pista, 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.

Para determinar si las PA-DSS se aplican a una aplicación de pago determinada, consulte la Guía del programa PA-DSS que se encuentra en www.pcisecuritystandards.org.

Aplicabilidad de las PCI DSS a los proveedores de aplicaciones de pago

Es posible que las PCI DSS no se apliquen directamente a proveedores de aplicaciones de pago si el proveedor almacena, procesa o transmite datos del titular de la tarjeta, o tiene acceso a los datos del titular de la tarjeta de sus clientes (por ejemplo, en la función de un proveedor de servicios).

Alcance de los requisitos de las PCI DSS

Los requisitos de seguridad de las PCI DSS se aplican a todos los componentes del sistema incluidos en el entorno de datos del titular de la tarjeta o conectados a este. El CDE (entorno de datos del titular de la tarjeta) consta de personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. El término “componentes del sistema” incluye dispositivos de red, servidores, dispositivos informáticos y aplicaciones. Los componentes del sistema incluyen, a modo de ejemplo:

- Sistemas que ofrecen servicios de seguridad (por ejemplo, servidores de autenticación), que facilitan la segmentación (por ejemplo, *firewalls* internos) o que pueden afectar la seguridad del CDE (por ejemplo, servidores de resolución de nombres o de redireccionamiento web).
- Componentes de virtualización, como máquinas virtuales, interruptores/routers virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores.
- Los componentes de red incluyen, a modo de ejemplo, *firewalls*, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de red y otras aplicaciones de seguridad.
- Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, bases de datos, autenticación, correo electrónico, proxy, NTP (protocolo de tiempo de red) y DNS (servidor de nombre de dominio).
- Aplicaciones, que abarcan todas las aplicaciones compradas y personalizadas, incluso las aplicaciones internas y externas (por ejemplo, Internet).
- Cualquier otro componente o dispositivo ubicado en el CDE o conectado a este.

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 deberá confirmar la exactitud del alcance de las PCI DSS al identificar todas las ubicaciones y los flujos de datos del titular de la tarjeta, e identificar todos los sistemas a los que se conectan o, si están en riesgo, podrían afectar al CDE (por ejemplo, los servidores de autenticación) para garantizar que se incluyan en el alcance de las PCI DSS. Todos los tipos de sistemas y ubicaciones deberán considerarse como parte del proceso de alcance, incluidos los sitios de copia de seguridad/recuperación y los sistemas de conmutación por error.

Para confirmar la exactitud del CDE definido, realice lo siguiente:

- La entidad evaluada identifica y documenta la existencia de todos los datos del titular de la tarjeta en su entorno, con la finalidad de verificar que no haya datos del titular de la tarjeta fuera del 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 del titular de la tarjeta encontrados están dentro del alcance de la evaluación de las PCI DSS y forman parte del CDE. Si la entidad identifica los datos que no están actualmente en el CDE, se deberán eliminar de manera segura, migrar al CDE actualmente definido o al CDE redefinido para incluir estos datos.

La entidad retiene la documentación que muestra cómo se determinó el alcance de las PCI DSS. La documentación se conserva para la revisión por parte de los asesores o como referencia durante la siguiente actividad anual de confirmación del alcance de las PCI DSS.

En cada evaluación de las PCI DSS, el asesor debe validar que el alcance de la evaluación esté correctamente definido y documentado.

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 enfáticamente como un método que puede disminuir lo siguiente:

- 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. Para considerarlo fuera de alcance para las PCI DSS, el componente del sistema debe estar correctamente aislado (segmentado) del CDE de manera tal que si el componente del sistema fuera de alcance está en riesgo no afecte la seguridad del CDE.

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 ciertos 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 la empresa/componentes del sistema proporciona más información sobre el efecto que la segmentación y el muestreo de la red sobre el alcance de la 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 una WLAN (red de acceso local inalámbrica) forma parte del entorno de datos de los titulares de tarjetas o está conectada a este, es necesario aplicar e implementar los requisitos de las PCI DSS y los procedimientos de pruebas para entornos inalámbricos (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.

Uso de proveedores de servicios externos/tercerización

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.

Las partes deben identificar con claridad los servicios y los componentes del sistema que estén dentro del alcance de la evaluación de las PCI DSS del proveedor de servicios, los requisitos específicos de las PCI DSS cubiertos por el proveedor de servicios y cualquier otro requisito que los clientes del proveedor de servicios deban incluir en las revisiones de las PCI DSS. Por ejemplo, un proveedor de *hosting* gestionado deberá definir, claramente, cuáles de las direcciones IP se analizarán como parte del proceso de análisis trimestral de vulnerabilidades y cuáles son las direcciones IP que el cliente debe incluir en sus propios análisis trimestrales.

Los proveedores de servicios son responsables de demostrar el cumplimiento de la PCI DSS, y las marcas de pago pueden exigir que lo hagan. Los proveedores de servicios deberán contactar a su adquirente y/o marca de pago para determinar la validación adecuada del cumplimiento.

Los terceros proveedores de servicios tienen dos formas de validar el cumplimiento:

1) **Evaluación anual**: Los proveedores de servicios pueden realizar una o varias evaluaciones anuales de las PCI DSS por cuenta propia y proporcionar evidencia a sus clientes a fin de demostrar el cumplimiento; o
2) **Evaluaciones múltiples, bajo demanda**: Si no se someten a sus propias evaluaciones anuales de la PCI DSS, los proveedores de servicios deben someterse a evaluaciones a solicitud de sus clientes y/o participar en cada una de las revisiones de la PCI DSS de sus clientes, proporcionando los resultados de cada revisión a sus respectivos clientes

Si el tercero lleva a cabo su propia evaluación de las PCI DSS, debe proporcionarles a los cliente la evidencia necesaria que corrobore que el alcance de la evaluación de las PCI DSS del proveedor de servicios cubre los servicios correspondientes al cliente y que se examinaron e implementaron los requisitos de las PCI DSS pertinentes. El tipo de evidencia específica que el proveedor de servicios les proporcione a los clientes dependerá de los acuerdos o contratos implementados entre dichas partes. Por ejemplo, proporcionar la AOC (atestación de cumplimiento) o las secciones relevantes del ROC (informe sobre cumplimiento) del proveedor de servicios (redactado para proteger la información confidencial) puede ser útil para proporcionar toda la información o parte de esta.

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.*

Mejores prácticas para implementar las PCI DSS en los procesos habituales

A fin de garantizar que los controles de seguridad se sigan implementando correctamente, las PCI DSS deberán implementarse en las actividades BAU (habituales) como parte de la estrategia general de seguridad. Esto permite que la entidad supervise constantemente la eficacia de los controles de seguridad y que mantenga el cumplimiento de las PCI DSS en el entorno entre las evaluaciones de las PCI DSS. Ejemplos de cómo incorporar las PCI DSS en las actividades BAU incluyen pero no se limitan a:

1. Monitorear los controles de seguridad, tales como *firewalls*, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM (supervisión de la integridad de archivos), antivirus, controles de acceso, etc., para asegurarse de que funcionan correctamente y según lo previsto.
2. Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes:
    - Restaurar el control de seguridad.
    - Identificar la causa de la falla.
    - Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad.
    - Implementar la mitigación (como procesos o controles técnicos) para evitar que la causa reaparezca.
    - Reanudar la supervisión del control de seguridad, quizás con una supervisión mejorada durante un tiempo a fin de verificar que el control funcione correctamente.
3. Revisar los cambios implementados en el entorno (por ejemplo, incorporación de nuevos sistemas, cambios en las configuraciones del sistema o la red) antes de finalizar el cambio y realizar las siguientes actividades:
    - Determinar el posible impacto en el alcance de las PCI DSS (por ejemplo, una nueva regla para los *firewalls* que permita la conectividad entre un sistema del CDE y otro sistema puede incorporar sistemas o redes adicionales al alcance de las PCI DSS).
    - Identificar los requisitos de las PCI DSS correspondientes a los sistemas y las redes afectados por los cambios (por ejemplo, si un nuevo sistema está dentro del alcance de las PCI DSS, se deberá configurar de acuerdo con las normas de configuración de sistemas, entre otros, FIM (supervisión de la integridad de archivos), AV (antivirus), parches, registros de auditorías, etc., y se deberá incorporar al programa trimestral de análisis de vulnerabilidades).
    - Actualizar el alcance de las PCI DSS e implementar los controles de seguridad, según sea necesario.
4. Si se implementan cambios en la estructura organizativa (por ejemplo, la adquisición o fusión de una empresa), se debe realizar una revisión formal del impacto en el alcance y en los requisitos de las PCI DSS.
5. Se deben realizar revisiones y comunicados periódicos para confirmar que los requisitos de las PCI DSS se siguen implementando y que el personal cumple con los procesos de seguridad. Estas revisiones periódicas deben abarcar todas las instalaciones y ubicaciones, en las que se incluyen tiendas minoristas, centros de datos, etc., e incluir la revisión de los componentes del sistema (o muestras de los componentes del sistema) a fin de verificar que siguen implementados los requisitos de las PCI DSS, por ejemplo, normas de configuración implementadas, parches y AV (antivirus) actualizados, registros de auditorías revisados y así sucesivamente. La entidad debe determinar la frecuencia de las revisiones periódicas en función del tamaño y de la complejidad del entorno.

Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de *firewall*, etc., para ayudar a la entidad a prepararse para la siguiente evaluación sobre cumplimiento.

6. Revisar las tecnologías de hardware y software, al menos, una vez al año para confirmar que el proveedor las sigue admitiendo y que pueden satisfacer los requisitos de seguridad de la entidad, incluida la PCI DSS. Si se detecta que el proveedor ya no puede admitir las tecnologías o que no pueden satisfacer las necesidades de seguridad de la entidad, la entidad debe preparar un plan de recuperación que incluya el reemplazo de la tecnología si fuera necesario.

Además de las prácticas anteriores, las organizaciones también deben considerar la opción de separar las tareas de las funciones de seguridad de modo que las funciones de seguridad y auditorías sean independientes de las funciones operativas. En entornos en los que una persona desempeña varias funciones (por ejemplo, operaciones de administración y seguridad), las tareas se deben asignar de manera tal que ninguna persona tenga control completo de un proceso sin un punto de verificación independiente. Por ejemplo, las tareas de configuración y de aprobación de cambios se pueden asignar a dos personas distintas.

Nota: *Para algunas entidades, estas mejores prácticas también son requisitos para garantizar el cumplimiento continuo de la PCI DSS. Por ejemplo, la PCI DSS incluye estos principios en algunos requisitos, y la Validación suplementaria de las entidades designadas (Anexo A3 de la PCI DSS) exige que las entidades designadas validen estos principios.*

Todas las organizaciones deberán considerar la implementación de estas mejores prácticas en su entorno, aun cuando no se requiere que la organización las valide.

Para los asesores: Muestreo de instalaciones de la empresa/componentes del sistema

El muestreo es una opción con la que cuentan los asesores para simplificar los procesos de evaluación que tienen una gran cantidad de instalaciones de la empresa o de componentes del sistema.

Aunque un asesor puede obtener muestras de las instalaciones de la empresa/componentes del sistema como parte de la revisión de cumplimiento de las PCI DSS de la entidad, la entidad no puede implementar los requisitos de las PCI DSS solamente a la muestra del entorno (por ejemplo, los requisitos para los análisis trimestrales de vulnerabilidades se implementan en todos los componentes del sistema). De igual manera, no está permitido que el asesor solo revise el cumplimiento de los requisitos de las PCI DSS de una muestra.

Después de analizar el alcance global y la complejidad del entorno que se está evaluando, el asesor puede seleccionar, de manera independiente, muestras representativas de instalaciones de la empresa/componentes del sistema a fin de evaluar el cumplimiento de los requisitos de las PCI DSS por parte de la entidad. 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 los tipos y las ubicaciones de las instalaciones de la empresa, así como todos los tipos de componentes del sistema dentro de las instalaciones de la empresa seleccionadas. Las muestras deben ser suficientemente grandes para proporcionar al asesor la seguridad de que los controles se implementaron de la manera esperada.

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 de la empresa seleccionada, incluya distintos sistemas operativos, funciones y aplicaciones que correspondan al área que se está evaluando.

En cada instalación de la empresa, por ejemplo, el asesor podría definir una muestra para incluir los servidores Sun que operan con Apache, 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 los servidores Linux que operan con MySQL. Si todas las aplicaciones operan con la misma versión de un sistema operativo (por ejemplo, Windows 7 o Solaris 10), la muestra deberá incluir una variedad de aplicaciones (por ejemplo, servidores de base de datos, servidores 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 se implementan procesos y controles estandarizados y centralizados de seguridad y operativos para las PCI DSS que garanticen uniformidad y que debe seguir cada instalación de la empresa/componente del sistema, la muestra puede ser menor de lo que sería necesario si no existieran procesos o 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. El asesor debe verificar que los controles estandarizados y centralizados estén implementados y que funcionen correctamente.

- 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.
- Las muestras de los componentes del sistema deben incluir todos los tipos y las combinaciones que estén en uso. Por ejemplo, en el caso de que se realicen muestras de aplicaciones, la muestra debe incluir todas las versiones y plataformas de cada tipo de aplicación.

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 la empresa/componentes del sistema

Los asesores deben revalidar la justificación del muestreo para cada evaluación. Si se utiliza el muestreo, se deben seleccionar diferentes muestras de instalaciones de la empresa 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 información sobre los “controles de compensación”, consulte los *Anexos B* y *C* mencionados anteriormente.

Instrucciones y contenido del informe sobre cumplimiento

Las instrucciones y el contenido del ROC (informe sobre cumplimiento) se proporcionan en la *Plantilla para crear informes ROC de la PCI DSS*.

La *Plantilla para crear informes ROC de las PCI DSS* se debe usar como la plantilla para crear el *informe sobre 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 o con el adquiriente para establecer los requisitos y las instrucciones del informe.

Proceso de evaluación de las PCI DSS

El proceso de evaluación de la PCI DSS incluye la finalización de los siguientes pasos:

1. Confirmar el alcance de la evaluación de las PCI DSS.
2. Llevar a cabo la evaluación de las PCI DSS del entorno según los procedimientos de pruebas de cada requisito.
3. Complete el informe correspondiente de la evaluación (es decir, el *SAQ* [cuestionario de autoevaluación] o el ROC [informe sobre cumplimiento]), que incluye la documentación de todos los controles de compensación, de acuerdo con la guía y las instrucciones de la PCI correspondientes.
4. Complete la Declaración de cumplimiento para Proveedores de servicios o Comerciantes, según corresponda, en su totalidad. Las Atestaciones de cumplimiento están disponibles en el sitio web de PCI SSC.
5. Presente el SAQ o el ROC y la Atestación de cumplimiento junto con cualquier otro documento solicitado, como los informes de análisis de ASV (proveedores aprobados de escaneo) al adquiriente (en el caso de comerciantes), a la marca de pago o a otro solicitante (en el caso de proveedores de servicios).
6. Si es necesario, realice la remediación para abordar los requisitos que no están implementados, y presentar un informe actualizado.

Versiones de la PCI DSS

A partir de la fecha de publicación del presente documento, la PCI DSS v3.2 es válida hasta el 31 de diciembre de 2018, después de lo cual se retira. Todas las validaciones de la PCI DSS después de esta fecha deben ser a la PCI DSS v3.2.1 o posterior.

La siguiente tabla ofrece un resumen de las versiones de la PCI DSS y sus fechas relevantes.[6]

Versión	Publicado	Retirado
PCI DSS, versión 3.2.1 (Este documento)	Mayo de 2018	Por determinarse
PCI DSS, versión 3.2	Abril de 2016	31 de diciembre de 2018

[6] Sujeto a cambios después del lanzamiento de una nueva versión de la PCI DSS.

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

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

- **Requisitos de las PCI DSS**: Esta columna define los requisitos de las normas de seguridad de datos; el cumplimiento de las PCI DSS se validará en comparación con estos requisitos.
- **Procedimientos de pruebas:** Esta columna muestra los procesos que el asesor debe seguir a los efectos de validar que los requisitos de las PCI DSS "se hayan implementado" y cumplido.
- **Guía:** Esta columna describe la meta o el objetivo de seguridad de cada requisito de las PCI DSS. Esta columna es solo una guía y su finalidad es ayudar a comprender el propósito de cada requisito. La guía de esta columna no reemplaza ni extiende los requisitos ni los procedimientos de prueba de la PCI DSS.

Nota: *Los requisitos de las PCI DSS no se deben considerar "implementados" si los controles no se han implementado aún o si están programados para completarse en el futuro. Después de que la entidad haya corregido los puntos sujetos a control o no implementados, el asesor volverá a evaluarlos a los efectos de validar que se realizó la corrección y que se cumplieron todos los requisitos.*

Consulte los siguientes recursos (disponibles en el sitio web de PCI SSC) para documentar la evaluación de las PCI DSS:

- *Para obtener instrucciones sobre cómo completar el ROC, consulte la* Plantilla para crear informes ROC de las PCI DSS.
- *Para obtener instrucciones sobre cómo completar el SAQ, consulte las* Instrucciones y directrices del SAQ de las PCI DSS.
- *Para obtener instrucciones sobre cómo presentar los informes de validación sobre cumplimiento de las PCI DSS, consulte* las Atestaciones de cumplimiento de las PCI DSS.

Desarrolle y mantenga redes y sistemas seguros.

Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta

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 las redes internas confidenciales de una entidad. El entorno de datos de los titulares de tarjetas 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 computadoras.

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

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
1.1 Establezca e implemente normas de configuración para *firewalls* y routers que incluyan lo siguiente:	**1.1** Inspeccione las normas de configuración de *firewalls* y routers y otros documentos especificados a continuación para verificar el cumplimiento e implementación de las normas.	Los *firewalls* y los routers son componentes clave de la arquitectura que controla la entrada a y la salida de la red. Estos dispositivos son unidades de software o hardware que bloquean el acceso no deseado y administran el acceso autorizado hacia dentro y fuera de la red. Las normas y los procedimientos de configuración ayudarán a garantizar que la primera línea de defensa de la organización en la protección de sus datos mantenga su solidez.
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.a** Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente: • Conexiones de red • Cambios en las configuraciones de *firewalls* y routers	La implementación y la documentación de un proceso para aprobar y probar todas las conexiones y cambios de los *firewalls* y los routers ayudarán a prevenir problemas de seguridad causados por una configuración errónea de la red, del router o del *firewall*. Sin las pruebas y la aprobación formal de los cambios, es posible que no se actualicen los registros de los cambios, lo que podría generar discrepancias entre los documentos de la red y la configuración real.
	1.1.1.b Para obtener una muestra de las conexiones de red, entreviste al personal responsable y revise los registros para verificar que se hayan aprobado y probado las conexiones de red.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	1.1.1.c Identifique una muestra de los cambios reales realizados en las configuraciones de *firewalls* y routers, compárela con los registros de cambio y entreviste al personal responsable para verificar que los cambios se hayan probado y aprobado.	
1.1.2 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.	**1.1.2.a** Revise los diagramas y observe las configuraciones de red para verificar que exista un diagrama de red actual que documente todas las conexiones con los datos de los titulares de tarjetas, incluso las redes inalámbricas.	Los diagramas de red describen cómo están configuradas las redes e identifican la ubicación de todos los dispositivos de la red. Sin los diagramas de red actuales, es posible que se omitan los dispositivos y se excluyan de manera accidental de los controles de seguridad implementados para las PCI DSS, por lo tanto, quedan vulnerables.
	1.1.2.b Entreviste al personal responsable para verificar que el diagrama esté actualizado.	
1.1.3 El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.	**1.1.3** Revise el diagrama de flujo de datos y entreviste al personal para verificar lo siguiente en el diagrama: • Muestra los flujos de datos de titulares de tarjetas entre los sistemas y las redes. • Se mantiene al día y está actualizado según los cambios implementados en el entorno.	El diagrama de flujo de los datos de titulares de tarjetas identifica la ubicación de todos los datos de titulares de tarjetas que se almacenan, procesan o transmiten dentro de la red. Los diagramas de flujo de datos de la red y de los titulares de tarjetas ayudan a la organización a entender y llevar un registro del alcance de su entorno al mostrar cómo circulan los datos de titulares de tarjetas entre las redes y entre los sistemas y dispositivos individuales.
1.1.4 Requisitos para tener un *firewall* en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	**1.1.4.a** Revise las normas de configuración de *firewalls* y controle que incluyan los requisitos para tener un *firewall* en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	El uso de un *firewall* en cada conexión de Internet entrante (y saliente) de la red y entre cualquier DMZ (zona desmilitarizada) y la red interna le permite a la organización supervisar, controlar el acceso y minimizar las posibilidades de que una persona malintencionada acceda a la red interna mediante una conexión sin protección.
	1.1.4.b Verifique que el diagrama de red actual concuerde con las normas de configuración de *firewalls*.	
	1.1.4.c Revise las configuraciones de red para verificar que haya un *firewall* en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna, de acuerdo con las normas de configuración documentadas y los diagramas de red.	
1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.	**1.1.5.a** Verifique que las normas de configuración de *firewalls* y routers incluyan la descripción de los grupos, las funciones y las responsabilidades para la administración de los componentes de la red.	Mediante la descripción de las funciones y la asignación de responsabilidades, el personal sabe quién está a cargo de la seguridad de todos los componentes de la red y aquellas personas encargadas de administrar los componentes saben cuál es su responsabilidad. Si no se asignan formalmente las funciones y las responsabilidades, es posible que los dispositivos queden sin supervisión.
	1.1.5.b Entreviste al personal responsable de administrar los componentes de la red para confirmar que las funciones y las responsabilidades se hayan asignado según lo documentando.	
1.1.6 Documentación y justificación de negocio para el uso de todos los	**1.1.6.a** Verifique que las normas de configuración de *firewalls* y routers incluyan una lista documentada de todos los	Con frecuencia se producen exposiciones debido a que los servicios y puertos no se utilizan o a

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros.	servicios, protocolos y puertos, incluida la justificación comercial y la aprobación para cada una. **1.1.6.b** Identifique los servicios, protocolos y puertos inseguros permitidos y verifique que se hayan documentado las funciones de seguridad de cada servicio. **1.1.6.c** Revise las configuraciones de *firewalls* y routers para verificar que se hayan implementado las funciones de seguridad para cada servicio, protocolo y puerto inseguros.	que no son seguros, ya que estos, por lo general, tienen vulnerabilidades conocidas y muchas organizaciones no implementan parches para las vulnerabilidades de los servicios, protocolos y puertos que no se utilizan (incluso estando presentes las vulnerabilidades). Mediante la definición y la documentación precisas de los servicios, protocolos y puertos necesarios para la empresa, las organizaciones pueden asegurarse de que se inhabiliten o eliminen el resto de los servicios, protocolos y puertos. Las aprobaciones deberán ser concedidas por personal independiente del personal que maneja la configuración. Si los servicios, protocolos o puertos inseguros son necesarios para la empresa, la organización debe entender y aceptar el riesgo que supone el uso de estos protocolos, además, se debe justificar el uso del protocolo y documentar e implementar las funciones de seguridad que permiten utilizar estos protocolos de manera segura. Si estos servicios, protocolos o puertos inseguros no son necesarios para la empresa, se deben inhabilitar o eliminar. Para obtener una guía sobre los servicios, protocolos o puertos que se consideran inseguros, consulte las normas y la guía de la industria (por ejemplo, NIST, ENISA, OWASP, etc.)
1.1.7 Requisito de la revisión de las normas de *firewalls* y routers, al menos, cada seis meses.	**1.1.7.a** Verifique que las normas de configuración de *firewalls* y routers soliciten la revisión de las reglas, al menos, cada seis meses. **1.1.7.b** Examine la documentación relacionada con las revisiones de las reglas y entreviste al personal responsable para verificar si las reglas se revisan, al menos, cada seis meses.	Esta revisión le brinda a la organización la oportunidad de eliminar todas las reglas innecesarias, desactualizadas o incorrectas, al menos, cada seis meses y de garantizar que todos los conjuntos de reglas otorguen permiso solo a los servicios y puertos autorizados que coincidan con las justificaciones de negocio documentadas. Las organizaciones que implementan numerosos cambios en las reglas de *firewalls* y routers deben considerar la opción de realizar revisiones más frecuentes a fin de asegurarse de que las reglas satisfagan las necesidades de la empresa.
1.2 Desarrolle configuraciones para *firewalls* y routers que restrinjan las conexiones entre redes no confiables y	**1.2** Revise las configuraciones de *firewalls* y routers y realice las siguientes acciones para verificar que se restringen las conexiones entre redes no confiables y todo componente del	Es fundamental instalar protección para la red entre la red interna confiable y cualquier red no confiable que sea externa o esté fuera de la

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
cualquier componente del sistema en el entorno de los datos de titulares de tarjetas. ***Nota:*** *Una "red no confiable" es toda red externa a las redes que pertenecen a la entidad en evaluación o que excede la capacidad de control o administración de la entidad.*	sistema en el entorno de datos de titulares de tarjetas:	capacidad de control y administración de la entidad. No implementar esta medida correctamente deja a la entidad expuesta al acceso no autorizado por parte de personas malintencionadas o un software malintencionado. Para que la funcionalidad del *firewall* sea eficaz, debe estar correctamente configurado para controlar o limitar el tráfico desde y hacia la red de la entidad.
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.	**1.2.1.a** Revise las normas de configuración de *firewalls* y routers para verificar que identifican el tráfico entrante y saliente necesario para el entorno de datos de titulares de tarjetas.	La evaluación de todas las conexiones entrantes y salientes brinda la oportunidad de inspeccionar y limitar el tráfico según las direcciones de origen/destino, previniendo así el acceso no filtrado entre entornos confiables y no confiables. Este requisito busca impedir que personas malintencionadas accedan a la red de la entidad a través de direcciones IP no autorizadas o que se utilicen servicios, protocolos o puertos sin autorización (por ejemplo, para enviar datos que hayan obtenido desde dentro de la red de la entidad hacia un servidor no confiable). Implementar una regla que niegue todo el tráfico entrante y saliente que no sea específicamente necesario ayuda a evitar agujeros inadvertidos que permitirán la entrada y salida de tráfico fortuito y potencialmente peligroso.
	1.2.1.b Revise las configuraciones de *firewalls* y routers para verificar que el tráfico entrante y saliente esté restringido a la cantidad necesaria para el entorno de datos de titulares de tarjetas.	
	1.2.1.c Revise las configuraciones de *firewalls* y routers para verificar que todo tráfico entrante y saliente se niegue de manera específica, por ejemplo, mediante 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.a** Revise los archivos de configuración del router para verificar que están protegidos contra el acceso no autorizado.	Si bien los archivos de configuración del router en ejecución (o activo) incluyen los parámetros actuales de configuración seguros, los archivos de inicio (que se usan cuando el router realiza un reinicio) se deben actualizar con los mismos parámetros de configuración segura para garantizar que estos parámetros se aplicarán cuando se ejecute la configuración de inicio. Debido a que los archivos de configuración de inicio solo se ejecutan ocasionalmente, muchas veces quedan en el olvido y no se actualizan. Cuando un router realiza un reinicio y carga una configuración de inicio que no se actualizó con los mismos parámetros de configuración segura que los de la configuración en ejecución, se pueden producir reglas más débiles que permitan que personas malintencionadas accedan a la red.
	1.2.2.b Revise las configuraciones del router y verifique que estén sincronizadas, por ejemplo, que la configuración en ejecución (o activa) coincida con la configuración de inicio (que se usa cuando la máquina se reinicia).	
1.2.3 Instale *firewalls* de perímetro entre las redes inalámbricas y el	**1.2.3.a** Revise las configuraciones de *firewalls* y routers, y verifique que se hayan instalado *firewalls* de perímetro entre	La implementación y explotación conocida (o desconocida) de tecnología inalámbrica dentro de

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
entorno de datos del titular de la tarjeta y configure estos *firewalls* para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	las redes inalámbricas y el entorno de datos del titular de la tarjeta. **1.2.3.b** Verifique que los *firewalls* nieguen o, si el tráfico es necesario para fines comerciales, permitan solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	una red constituyen una ruta común para que personas malintencionadas obtengan acceso a la red y a datos de titulares de tarjetas. Si una red o un dispositivo inalámbrico se instala sin el conocimiento de la entidad, una persona malintencionada podría ingresar en la red fácilmente y sin ser vista. Si los *firewalls* no restringen el acceso de las redes inalámbricas al CDE (entorno de datos del titular de la tarjeta), las personas malintencionadas que obtengan acceso no autorizado a la red inalámbrica se pueden conectar fácilmente al CDE (entorno de datos del titular de la tarjeta) y poner en riesgo la información de las cuentas. Se deben instalar *firewalls* entre las redes inalámbricas y el CDE, independientemente del propósito del entorno al que esté conectada la red inalámbrica. Esto puede incluir, a modo de ejemplo, redes corporativas, tiendas minoristas, redes de huéspedes, almacenes, etc.
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** Revise las configuraciones de *firewalls* y routers, que incluye, entro otros, 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, y realice lo siguiente a fin de determinar que no exista un acceso directo entre la Internet y los componentes del sistema en el segmento de red interna de los titulares de tarjeta:	Si bien puede haber razones legítimas para permitir conexiones que no son de confianza en los sistemas de la DMZ (por ejemplo, permitir el acceso del público a un servidor web), dichas conexiones nunca deben concederse a los sistemas de la red interna. El objetivo de un *firewall* es administrar y controlar todas las conexiones entre los sistemas públicos y los sistemas internos, especialmente aquellos que almacenan, procesan o transmiten datos del titular de la tarjeta. Si se permite el acceso directo entre los sistemas públicos y el CDE, se burlan las protecciones que ofrece el *firewall* y se pueden poner en riesgo los componentes del sistema que almacenan los datos del titular de la tarjeta.
1.3.1 Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	**1.3.1** Revise las configuraciones de *firewalls* y routers, y verifique que se haya implementado una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	La DMZ se refiere a la parte de la red que administra las conexiones entre la Internet (u otras redes no confiables) y los servicios que una organización necesita poner a disposición del público (como un servidor web). El objetivo de esta funcionalidad es impedir el acceso de personas malintencionadas a la red interna de la organización a través de Internet o que se utilicen servicios, protocolos o puertos sin
1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	**1.3.2** Revise las configuraciones de *firewalls* y routers, y verifique que se restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
		autorización.
1.3.3 Implementar medidas antisuplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna).	**1.3.3** Revise las configuraciones de *firewalls* y routers, y verifique que se hayan implementado medidas contra la suplantación, por ejemplo, las direcciones internas no se pueden transferir de Internet a la DMZ**.**	Generalmente, un paquete contiene la dirección IP de la computadora desde la cual se envió originalmente, por lo tanto, las otras computadoras de la red saben de dónde proviene el paquete. Las personas malintencionadas intentarán suplantar (o imitar) la dirección IP de destino para que el sistema de destino crea que el paquete proviene de una fuente confiable. Filtrar los paquetes provenientes de la red ayuda, entre otras cosas, a evitar la "suplantación" de los paquetes para que parezcan que provienen de la red interna de la organización.
1.3.4 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.	**1.3.4** Revise las configuraciones de *firewalls* y routers, y verifique que el tráfico saliente proveniente del entorno de datos del titular de la tarjeta a Internet esté explícitamente autorizado.	Todo el tráfico saliente del entorno de datos del titular de la tarjeta se debe evaluar para garantizar que respete las reglas establecidas y autorizadas. Las conexiones se deben inspeccionar a fin de limitar el tráfico sólo a las comunicaciones autorizadas (por ejemplo, al limitar direcciones/puertos de origen/destino y/o bloquear contenido).
1.3.5 Solo permita conexiones "establecidas" en la red.	**1.3.5** Revise las configuraciones de *firewalls* y routers para verificar que los *firewalls* permiten solo conexiones establecidas en la red interna y que niegan cualquier conexión entrante que no está asociada con una sesión previamente establecida.	Un *firewall* que mantiene el "estado" de cada conexión que pasa por el *firewall* conoce si una aparente respuesta a una conexión anterior es, en realidad, una respuesta válida autorizada (ya que conserva el estado de cada conexión) o si es tráfico malintencionado que intenta engañar al *firewall* para que permita la conexión.
1.3.6 Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.	**1.3.6** Revise las configuraciones de *firewalls* y routers, y verifique que los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) se encuentren en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.	Si los datos del titular de la tarjeta se encuentran en la DMZ (zona desmilitarizada), un atacante externo puede acceder a esta información con más facilidad porque hay menos capas que penetrar. Proteger con un *firewall* los componentes del sistema que almacenan los datos del titular de la tarjeta en una zona de red interna que está segregada desde la DMZ (zona desmilitarizada) y otras redes no confiables puede evitar que el tráfico de red no autorizado llegue a los componentes del sistema. ***Nota:*** *El objetivo de este requisito no es aplicarlo al almacenamiento temporal de los datos del titular de la tarjeta en una memoria volátil.*

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
1.3.7 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, los siguientes:* • *Traducción de Dirección de Red (NAT)* • *Ubicación de los servidores que contengan datos del titular de la tarjeta detrás de los servidores proxy/firewalls.* • *Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas,* • *Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas.*	**1.3.7.a** Revise las configuraciones de *firewalls* y routers, y verifique que se hayan implementado métodos para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde redes internas a Internet. **1.3.7.b** Entreviste al personal, revise la documentación y verifique que no se autorice la divulgación de ninguna dirección IP privada ni de información de enrutamiento a entidades externas.	Restringir la divulgación de direcciones IP internas o privadas resulta fundamental para evitar que un hacker adquiera las direcciones IP de la red interna y utilice esa información para acceder a la red. Los métodos utilizados para cumplir con el objetivo de este requisito pueden variar según la tecnología de red utilizada. Por ejemplo, los controles utilizados para cumplir con este requisito en las redes IPv4 difieren de los de las redes IPv6.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
1.4 Instale software de *firewall* personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder al CDE. Las configuraciones de *firewall* (o equivalente) incluyen: • Se definen los ajustes específicos de configuración. • El *firewall* personal (o funcionalidad equivalente) se ejecuta de forma activa. • El *firewall* personal (o una funcionalidad equivalente) no puede ser alterado por los usuarios de los dispositivos informáticos portátiles.	**1.4.a** Revise **las** políticas y las normas de configuración para verificar lo siguiente: • Se debe incluir software de *firewall* personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usen para acceder al CDE. • Los ajustes específicos de configuración se definen para cada software de *firewall* personal (o funcionalidad equivalente). • El *firewall* personal (o una funcionalidad equivalente) está configurado para ejecutarse de forma activa. • El *firewall* personal (o una funcionalidad equivalente) está configurado para no poder ser alterado por los usuarios de los dispositivos informáticos portátiles. **1.4.b** Inspeccione una muestra de dispositivos móviles de propiedad de la empresa y/o de los trabajadores para verificar que: • El *firewall* personal (o funcionalidad equivalente) está instalado y configurado de conformidad con los parámetros de configuración específicos de la empresa. • El *firewall* personal (o funcionalidad equivalente) se ejecuta de forma activa. • El *firewall* personal (o una funcionalidad equivalente) no puede ser alterado por los usuarios de los dispositivos informáticos portátiles.	Los dispositivos informáticos portátiles autorizados para conectarse a Internet desde afuera del *firewall* corporativo son más vulnerables a las amenazas basadas en Internet. El uso de una funcionalidad *firewall* (por ejemplo, hardware o software de *firewall* personal) ayuda a proteger los dispositivos contra ataques basados en Internet, los cuales pueden usar el dispositivo para obtener acceso a los datos y a los sistemas de la organización cuando el dispositivo se conecta nuevamente a la red. La organización determina los parámetros de configuración específicos del *firewall*. ***Nota:*** *El objetivo de este requisito es aplicarlo a las computadoras de los trabajadores y de la empresa. Los sistemas que la política corporativa no puede administrar introducen debilidades en el perímetro y brindan oportunidades que las personas malintencionadas pueden explotar. Permitir que sistemas no confiables se conecten al CDE de la organización puede generar el acceso de atacantes y otros usuarios malintencionados.*
1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los *firewalls* estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**1.5** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para administrar los *firewalls* cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar las políticas de seguridad y los procedimientos operativos para garantizar la continua administración de los *firewalls* y routers con el objetivo de evitar el acceso no autorizado a la red.

Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad

Las personas malintencionadas (externas e internas a una entidad), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para comprometer los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se determinan fácilmente por medio de información pública.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias **antes** de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, *los terminales de* POS *(*puntos de venta*)*, las aplicación de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.	**2.1.a** Escoja una muestra de los componentes del sistema e intente acceder a los dispositivos y aplicaciones (con la ayuda del administrador del sistema) con las cuentas y contraseñas predeterminadas por el proveedor y verifique que se hayan cambiado TODAS las contraseñas predeterminadas (incluso las de los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS [puntos de ventas], las cadenas comunitarias de SNMP [protocolo simple de administración de red]). (Utilice los manuales y las fuentes de los proveedores que se encuentran en Internet para encontrar las cuentas y las contraseñas proporcionadas por estos).	Las personas malintencionadas (externas e internas a la organización), por lo general, utilizan configuraciones predeterminadas por los proveedores, nombres de cuentas y contraseñas para poner en riesgo el software del sistema operativo, las aplicaciones y los sistemas donde están instalados. Debido a que estos parámetros predeterminados suelen publicarse y son conocidos en las comunidades de hackers, cambiar estas configuraciones contribuirá a que el sistema sea menos vulnerable a los ataques. Incluso si una cuenta predeterminada no se creó para usarse, cambiar la contraseña predeterminada por una contraseña única y sólida y, después, deshabilitar la cuenta, evitará que personas maliciosas vuelvan a habilitar la cuenta y accedan con la contraseña predeterminada.
	2.1.b Para la muestra de los componentes del sistema, verifique que todas las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los software de seguridad, las aplicaciones, los sistemas, los terminales de POS [puntos de ventas], SNMP [protocolo simple de administración de red], etc.) se hayan eliminado o deshabilitado.	
	2.1.c Entreviste al personal, revise la documentación de respaldo y verifique lo siguiente: • Se cambian todos los valores predeterminados por proveedores (incluidas las contraseñas predeterminadas de sistemas operativos, software que presta servicios de seguridad, cuentas de aplicaciones y sistemas, terminales de POS, cadenas de comunidad de protocolo simple de administración de red [SNMP], etc.) antes de instalar un sistema en la red. • Se cambian o inhabilitan las cuentas predeterminadas	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	innecesarias (incluidas las cuentas que usan sistemas operativos, software de seguridad, aplicaciones, sistemas, terminales de POS, SNMP, etc.) antes de instalar un sistema en la red.	
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 TODOS los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica al momento de la instalación, incluidas, a modo de ejemplo, las claves de cifrado inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias SNMP (protocolo simple de administración de red).	**2.1.1.a** Entreviste al personal y revise la documentación de respaldo para verificar lo siguiente: • Las claves de cifrado predeterminadas se cambiaron al momento de la instalación. • Las claves de cifrado se cambian cada vez que una persona que tenga conocimiento de estas cesa en sus funciones o se traslada a otro cargo en la empresa.	Si las redes inalámbricas no se implementan con suficientes configuraciones de seguridad (incluido el cambio de los parámetros predeterminados), los *sniffers* inalámbricos pueden espiar el tráfico, capturar datos y contraseñas de manera sencilla e ingresar en la red y atacarla fácilmente. Además, el protocolo de intercambio de claves de versiones anteriores de cifrado 802.11x (privacidad equivalente por cable o WEP) ha sido transgredido y puede inutilizar el cifrado. El firmware de los dispositivos se debe actualizar para admitir protocolos más seguros.
	2.1.1.b Entreviste al personal, revise las políticas y procedimientos y verifique lo siguiente: • Las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas se cambian al momento de la instalación. • Las frases/contraseñas predeterminadas de los puntos de accesos se cambian al momento de la instalación.	
	2.1.1.c Revise la documentación proporcionada por el proveedor, inicie sesión en los dispositivos inalámbricos con la ayuda del administrador del sistema y verifique lo siguiente: • No se usan las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas. • No se usan las contraseñas/frases predeterminadas de los puntos de acceso.	
	2.1.1.d Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que el firmware de los dispositivos inalámbricos se actualice a fin de admitir el cifrado sólido para lo siguiente: • Autenticación en redes inalámbricas. • Transmisión en redes inalámbricas.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	2.1.1.e Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que se hayan cambiado los otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 sean coherentes con las normas de protección de sistemas 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** Revise las políticas, entreviste al personal y verifique que las normas de configuración de sistemas se actualicen a medida que se identifiquen nuevas vulnerabilidades, tal como se define en el Requisito 6.1. **2.2.c** Revise las políticas, entreviste al personal y verifique que se apliquen las normas de configuración de sistemas al configurar y comprobar que se instalaron nuevos sistemas antes de instalar un sistema en la red. **2.2.d** Verifique que las normas de configuración de sistemas incluyan los siguientes procedimientos para todos los tipos de componentes del sistema: • Cambiar los valores predeterminados de los proveedores y eliminar las cuentas predeterminadas innecesarias. • Implementar solo una función principal por servidor a fin de evitar que coexistan funciones que requieran diferentes niveles de seguridad en el mismo servidor. • Habilitar solo los servicios, protocolos, *daemons*, etc., necesarios, según lo requiera la función del sistema. • Implementar funciones de seguridad adicionales para los servicios, protocolos o *daemons* requeridos que no se consideren seguros. • Configurar los parámetros de seguridad del sistema para evitar el uso indebido. • Eliminar todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.	Existen debilidades conocidas en muchos sistemas operativos, bases de datos y aplicaciones de empresas, así como también existen maneras de configurar estos sistemas a fin de corregir las vulnerabilidades de seguridad. A fin de ayudar a quienes no son expertos en seguridad, algunas organizaciones especializadas han establecido recomendaciones y directrices para reforzar los sistemas, las cuales proporcionan consejos para corregir estas debilidades. Algunas fuentes para obtener información sobre las normas de configuración son las siguientes: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org y proveedores de productos. Las normas de configuración de sistemas deben estar actualizadas a fin de asegurar que las debilidades recientemente identificadas se corrijan antes de instalar un sistema en la red.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 solo una función principal por componente de sistema virtual.*	**2.2.1.a** Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones del sistema y verifique que se haya implementado solo una función principal en cada servidor. **2.2.1.b** Si se utilizan tecnologías de virtualización, inspeccione las configuraciones del sistema y verifique que se haya implementado una sola función principal por componente de sistema o dispositivo virtual.	Si las funciones de servidores que necesitan diferentes niveles de seguridad se encuentran en el mismo servidor, se reducirá el nivel de seguridad de las funciones que necesitan más seguridad debido a la presencia de funciones de menor seguridad. Además, las funciones del servidor que tengan un nivel de seguridad menor pueden introducir debilidades en otras funciones del mismo servidor. Al analizar las necesidades de seguridad de las diferentes funciones del servidor como parte de las normas de configuración de sistemas y de los procesos asociados, las organizaciones pueden garantizar que las funciones que necesitan diferentes niveles de seguridad no coexistan en el mismo servidor.
2.2.2 Habilite solo los servicios, protocolos y *daemons*, etc., necesarios, según lo requiera la función del sistema.	**2.2.2.a** Seleccione una muestra de los componentes del sistema, inspeccione los servicios del sistema, *daemons* y protocolos habilitados y verifique que solo se habiliten los servicios o protocolos necesarios. **2.2.2.b** Identifique los servicios, *daemons* o protocolos habilitados que no sean seguros, entreviste al personal y verifique que estén configurados de conformidad con las normas de configuración documentadas.	Tal como lo especifica el Requisito 1.1.6, existen numerosos protocolos que puede necesitar un negocio (o tener habilitados por opción predeterminada) que, habitualmente, utilizan personas malintencionadas para poner en riesgo una red. Incluir este requisito como parte de las normas de configuración y procesos relacionados de la organización garantiza que solo se habiliten los servicios o protocolos necesarios.
2.2.3 Implementar funciones de seguridad adicionales para los servicios, protocolos o *daemons* requeridos que no se consideren seguros.	**2.2.3** Inspeccione los parámetros de configuración y verifique que las funciones de seguridad se hayan documentado e implementado en todos los servicios, *daemons* o protocolos no seguros.	Habilitar las funciones de seguridad antes de implementar los nuevos servidores evitará que se instalen servidores con configuraciones inseguras en el entorno. Asegurarse de que todos los servicios, protocolos y *daemons* inseguros se protejan correctamente con las funciones de seguridad correspondientes dificulta más la tarea de las personas malintencionadas de aprovecharse de los puntos comunes de riesgo de la red. Consulte las normas de la industria y las mejores prácticas para obtener información sobre la criptografía sólida y los protocolos seguros (por ejemplo, NIST SP 800-52 y SP 800-57, OWASP, etc.) ***Nota:*** SSL/TLS temprana no se considera criptografía

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
		sólida y no puede utilizarse como control de seguridad, excepto por los terminales de POS POI que se pueden verificar como no susceptibles a cualquier vulnerabilidad conocida y los puntos de terminación a los que se conectan, según se define en el Anexo A2.
2.2.4 Configure los parámetros de seguridad del sistema para evitar el uso indebido.	**2.2.4.a** Entreviste a los administradores del sistema o a los gerentes de seguridad para verificar que conocen las configuraciones comunes de parámetros de seguridad de los componentes del sistema.	Las normas de configuración del sistema y los procesos relacionados deben abordar, específicamente, los valores de configuración y los parámetros de seguridad que tienen implicaciones de seguridad conocidas en cada sistema en uso. Para configurar los sistemas de manera segura, el personal responsable de la configuración o administración de sistemas debe conocer los parámetros y los valores específicos de seguridad del sistema.
	2.2.4.b Revise las normas de configuración de sistemas y verifique que incluyan los valores comunes de los parámetros de seguridad.	
	2.2.4.c Seleccione una muestra de los componentes del sistema e inspeccione los parámetros de seguridad comunes para verificar que se hayan configurado correctamente, según las normas de configuración.	
2.2.5 Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.	**2.2.5.a** Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones y verifique que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos, controladores, funciones, subsistemas, sistemas de archivos, etc.).	Las funciones innecesarias pueden ofrecer oportunidades adicionales para que personas malintencionadas accedan al sistema. Al eliminar las funciones innecesarias, las organizaciones pueden centrarse en proteger las funciones necesarias y eliminar el riesgo de que se exploten funciones desconocidas. Incluir esto en los procesos y en las normas para reforzar servidores aborda las implicaciones de seguridad específicas relacionadas con las funciones innecesarias (por ejemplo, eliminar/inhabilitar FTP o el servidor web si el servidor no realizará estas funciones).
	2.2.5.b. Revise la documentación y los parámetros de seguridad, y verifique que las funciones habilitadas estén documentadas y admitan la configuración segura.	
	2.2.5.c. Revise la documentación y los parámetros de seguridad, y verifique que solo la funcionalidad documentada esté presente en la muestra de componentes del sistema.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido.	**2.3** Seleccione una muestra de los componentes del sistema y verifique que el acceso administrativo que no sea de consola se cifre al realizar lo siguiente:	Si la administración que no es de consola (incluso la remota) no usa autenticación segura ni comunicaciones cifradas, la información confidencial a nivel administrativo u operativo (como contraseñas o ID del administrador) se puede revelar a un espía. Una persona malintencionada podría utilizar esta información para acceder a la red, hacerse pasar por administrador y hurtar datos. Los protocolos de texto no cifrado (como HTTP, telnet, etc.) no cifran el tráfico ni los detalles de inicio de sesión, por lo que un espía puede interceptar esta información fácilmente. Para que sea considerada una “criptografía sólida”, se deben implementar los protocolos reconocidos por la industria con el nivel de clave y la administración de claves adecuados según el tipo de tecnología utilizada. (Consulte la "criptografía sólida" en el *Glosario de términos, abreviaturas y acrónimos de la PCI DSS y PA-DSS,* y las normas y las mejores prácticas de la industria como NIST SP 800-52 y SP 800-57, OWASP, etc.) ***Nota:*** SSL/TLS temprana no se considera criptografía sólida y no puede utilizarse como control de seguridad, excepto por los terminales de POS POI que se pueden verificar como no susceptibles a cualquier vulnerabilidad conocida y los puntos de terminación a los que se conectan, según se define en el Anexo A2.
	2.3.a Observe a un administrador mientras inicia sesión en cada sistema y revise las configuraciones de los sistemas 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 los archivos de parámetros en los sistemas a fin de determinar que Telnet y otros comandos de inicio de sesión remotos inseguros no están disponibles para acceso sin consola.	
	2.3.c Observe a un administrador mientras inicia sesión en cada sistema y verifique que el acceso del administrador a cualquier interfaz de administración basada en la Web esté cifrado mediante una criptografía sólida.	
	2.3.d Revise la documentación del proveedor y entreviste al personal a fin de controlar que se implemente una criptografía sólida para la tecnología usada de acuerdo con las mejores prácticas de la industria y las recomendaciones del proveedor.	
2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS.	**2.4.a** Revise el inventario del sistema para verificar que haya una lista de componentes del hardware y del software con una descripción de la función/uso de cada componente.	Tener una lista actualizada de todos los componentes del sistema permitirá que la organización defina, de manera precisa y eficaz, el alcance de su entorno para implementar los controles de las PCI DSS. Sin un inventario, es posible que algunos de los componentes del sistema queden en el olvido y se excluyan, accidentalmente, de las normas de configuración de la organización.
	2.4.b Entreviste al personal y verifique que el inventario esté actualizado.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**2.5** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar las políticas de seguridad y los procedimientos operativos diarios para garantizar la continua administración de los parámetros predeterminados del proveedor y otros parámetros de seguridad a fin de evitar configuraciones inseguras.
2.6 Los proveedores de *hosting* compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el *Anexo A1: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting.*	**2.6** Lleve a cabo los procedimientos de pruebas desde **A.1.1** hasta **A.1.4** que se describen en el *Anexo A1: Requisitos adicionales de las PCI DSS para los proveedores de hosting compartido* en lo que respecta a la evaluación de las PCI DSS de los proveedores de *hosting* compartido para verificar que estos proveedores protejan el entorno y los datos que alojan las entidades (comerciantes y proveedores de servicios).	Se concibió pensando en los proveedores de servicio de *hosting* que proporcionan entornos de *hosting* compartidos para múltiples clientes en el mismo servidor. Cuando todos los datos se encuentran en el mismo servidor y bajo el control de un único entorno, con frecuencia, los parámetros de configuración de estos servidores compartidos no pueden ser administrados por clientes individuales. Esto permite que los clientes agreguen funciones y secuencias de comandos no seguros que afectan la seguridad de todos los demás entornos y, en consecuencia, facilita que personas malintencionadas pongan en riesgo los datos de un cliente y obtengan acceso a los datos de los demás clientes. Consulte el *Anexo A1* para obtener detalles de los requisitos.

Proteger los datos del titular de la tarjeta

Requisito 3: Proteger los datos almacenados del titular de la tarjeta

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. 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. También se deberían considerar otros métodos eficaces para proteger los datos almacenados oportunidades para mitigar posibles riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario; truncar los datos del titular de la tarjeta si no se necesita el PAN (número de cuenta principal) completo y no enviar el PAN (número de cuenta principal) utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea.

Consulte el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y de las PA-DSS* para obtener definiciones de “criptografía sólida” y otros términos de las PCI DSS.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta): • Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio • Requisitos de retención específicos para datos de titulares de tarjetas • Procesos para eliminar datos de manera cuando ya no se necesiten • Un proceso trimestral para identificar y eliminar, de manera segura, los datos	**3.1.a** Revise las políticas, los procedimientos y los procesos de retención y eliminación de datos y verifique que incluyen lo siguiente para todo el almacenamiento de los datos del titular de la tarjeta (CHD): • Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio. • Requisitos específicos para la retención de datos del titular de la tarjeta (por ejemplo, los datos del titular de la tarjeta se debe mantener durante X tiempo por Y razones de la empresa). • Eliminación segura de los datos del titular de la tarjeta cuando ya no son necesarios por motivos legales, reglamentarios o empresariales. • Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan los requisitos de retención definidos.	Una política formal para la retención de datos identifica los datos que se deben conservar, así como el lugar donde residen los datos, de modo que se puedan destruir o eliminar de manera segura cuando ya no sean necesarios. Los únicos datos del titular de la tarjeta que se pueden almacenar después de la autorización son el número de cuenta principal o PAN (que debe ser ilegible), la fecha de vencimiento, el nombre del titular de la tarjeta y el código de servicio. Es necesario saber dónde se encuentran los datos del titular de la tarjeta para poder conservarlos o eliminarlos correctamente cuando ya no sean necesarios. A fin de definir los requisitos de retención apropiados, una entidad primero debe entender las necesidades de su negocio, así como cualesquiera obligaciones

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
del titular de la tarjeta almacenados que excedan la retención definida.	**3.1.b** Entreviste al personal y verifique lo siguiente: • Todos los lugares donde se almacenan datos de titulares de tarjetas están incluidos en los procesos de retención y eliminación de datos. • Se implementa un proceso trimestral automático o manual para identificar y eliminar, de manera segura, los datos de titulares de tarjetas almacenados. • El proceso trimestral automático o manual se lleva a cabo en todas las ubicaciones de datos de titulares de tarjetas.	legales y regulatorias que se apliquen a su industria, y/o que se apliquen al tipo de dato que se retiene.
	3.1.c Para obtener una muestra de los componentes del sistema que almacenan datos del titular de la tarjeta: • Revise los archivos y los registros del sistema para verificar que los datos almacenados no superen los requisitos definidos en la política de retención de datos. • Observe el mecanismo de eliminación y verifique que los datos se eliminen de manera segura.	Identificar y eliminar los datos almacenados que hayan excedido el período de retención especificado evita la retención de datos innecesarios. Este proceso puede ser automático o manual, o una combinación de las dos opciones. Por ejemplo, se podría implementar un procedimiento programático (automático o manual) para encontrar y eliminar datos, o una revisión manual de las áreas de almacenamiento de datos. La implementación de métodos de eliminación seguros asegura que los datos no se puedan recuperar cuando ya no sean necesarios. ***¡Recuerde, si no los necesita, no los almacene!***
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos confidenciales de autenticación, convertir todos los datos en irrecuperables al finalizar el proceso de autorización. *Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos de autenticación confidenciales en los*	**3.2.a** En el caso de los emisores de tarjetas o las empresas que respaldan servicios de emisión y almacenan datos de autenticación confidenciales, revise las políticas y entreviste al personal para verificar que existe una justificación de negocio documentada para almacenar datos de autenticación confidenciales.	Los datos de autenticación confidenciales consisten en el contenido completo de la pista, los códigos o valores de validación de la tarjeta y los datos de PIN. ¡Se prohíbe el almacenamiento de datos confidenciales de autenticación después de la autorización! Estos datos son muy valiosos para las personas malintencionadas, ya que les permiten generar tarjetas de pago falsas y crear transacciones fraudulentas. Las entidades que emiten tarjetas de pago, que prestan o respaldan servicios de emisión crearán
	3.2.b En el caso de los emisores de tarjetas o las empresas que respaldan servicios de emisión y almacenan datos de autenticación confidenciales, revise los almacenamientos de datos y la configuración del sistema para verificar que los datos de autenticación confidenciales estén protegidos.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
siguientes casos: • *Si existe una justificación de negocio.* • *Si los datos se almacenan de forma segura.* Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3, establecidos a continuación:	**3.2.c** En el caso de otras entidades, si se reciben datos de autenticación confidenciales, revise las políticas y los procedimientos, y revise la configuración del sistema a fin de verificar que los datos no se conservan después de la autorización.	y controlarán, con frecuencia, los datos de autenticación confidenciales como parte de su tarea de emisión. A las compañías que realizan, facilitan o respaldan servicios de emisión se les permite almacenar datos confidenciales de autenticación SÓLO SI tienen una necesidad de negocio legítima de almacenar dichos datos. Cabe señalar que todos los requisitos de las PCI DSS rigen para los emisores, y que la única excepción para los emisores y procesadores emisores es que pueden retener datos si existe una razón legítima para hacerlo. Una razón legítima es aquella necesaria para el desempeño de la función proporcionada por el emisor y no, por conveniencia. Dichos datos se deben almacenar de manera segura y de conformidad con las PCI DSS y los requisitos específicos de las marcas de pago. *(continúa en la página siguiente)*
	3.2.d En el caso de otras entidades, si se reciben datos de autenticación confidenciales, revise los procedimientos y analice los procesos de eliminación segura de datos a fin de verificar que los datos sean irrecuperables.	Las entidades no emisoras no pueden retener datos confidenciales de autenticación después de la autorización.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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) después de la autorización. 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, revise 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 después de la autorización: • 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	Si se almacena el contenido completo de la pista, las personas malintencionadas que obtengan esos datos pueden reproducir tarjetas de pago y efectuar transacciones fraudulentas.
3.2.2 No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización.	**3.2.2** En el caso de la muestra de componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que el código o el valor de verificación de la tarjeta de tres o de cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no se almacene después de la autorización: • 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	El propósito del código de validación de las tarjetas es proteger las transacciones que se efectúan de manera no presencial, ya sean transacciones por Internet o MO/TO (correo o teléfono), en las que ni el consumidor ni la tarjeta están presentes. Si se hurtan estos datos, las personas malintencionadas pueden efectuar transacciones fraudulentas por Internet y transacciones MO/TO (correo o teléfono).

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.2.3 Después de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado.	**3.2.3** En el caso de la muestra de los componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que los PIN y los bloqueos de PIN cifrados no se almacenen después de la autorización: • 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	Sólo el propietario de la tarjeta o el banco emisor de la tarjeta deben conocer estos valores. Si se hurtan estos datos, personas malintencionadas pueden efectuar transacciones de débito basadas en PIN fraudulentas (por ejemplo, retiros de cajeros automáticos).
3.3 Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN. ***Nota**: Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).*	**3.3.a** Revise las políticas y los procedimientos escritos para ocultar las vistas de PAN (número de cuenta principal) para verificar lo siguiente: • Se documenta una lista de las funciones que necesitan acceso a más que los primeros seis o los últimos cuatro dígitos (incluye el PAN completo), junto con la necesidad empresarial legítima que justifique dicho acceso. • Se debe ocultar el PAN cuando aparezca para que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis y los últimos cuatro dígitos del PAN. • Todas las demás funciones que no estén específicamente autorizadas para ver PAN completos solo deben ver PAN ocultos. **3.3.b** Revise las configuraciones del sistema y verifique que las vistas del PAN (número de cuenta principal) estén disponibles solo para aquellos usuarios/funciones que tengan una necesidad comercial legítima y que el PAN (número de cuenta principal) esté oculto para el resto de las solicitudes.	La presentación de un PAN completo en pantallas de computadoras, recibos de tarjetas de pago, faxes o informes impresos puede facilitar la obtención y uso fraudulento de estos datos por parte de personas malintencionadas. Asegurarse de que solo aquellas personas que tengan una necesidad comercial legítima puedan ver el PAN (número de cuenta principal) completo minimiza el riesgo de que personas no autorizadas tengan acceso a los datos del PAN (número de cuenta principal). El enfoque de ocultamiento siempre deberá garantizar que solo se muestre el número mínimo de dígitos necesario para realizar una función comercial específica. Por ejemplo, si solo se necesitan los últimos cuatro dígitos para realizar una función comercial, enmascare el PAN para que las personas que realizan esa función solo puedan ver los últimos cuatro dígitos. A manera

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	3.3.c Revise las vistas del PAN (por ejemplo, en la pantalla o en recibos en papel) a fin de controlar que los PAN se oculten cuando muestren los datos del titular de la tarjeta, y que solo aquellos con una necesidad empresarial legítima puedan ver más que los primeros seis o los últimos cuatro dígitos del PAN.	de otro ejemplo, si una función necesita tener acceso al número de identificación bancaria (BIN) para fines de enrutamiento, quite el ocultamiento solo de los dígitos del BIN (tradicionalmente los primeros seis dígitos) durante esa función. Este requisito se relaciona con la protección del PAN (número de cuenta principal) *que se muestra* en pantallas, recibos impresos, impresiones, etc., y no se debe confundir con el Requisito 3.4 para la protección del PAN (número de cuenta principal) cuando *se almacena* en archivos, bases de datos, etc.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.4 Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos: • Valores hash de una vía basados en criptografía sólida (el hash debe ser del PAN completo) • Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) • *Tokens* y ensambladores de índices (los ensambladores se deben almacenar de manera segura). • Criptografía sólida con procesos y procedimientos asociados para la administración de claves. ***Nota:*** *Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash*	**3.4.a** Revise la documentación sobre el sistema utilizado para proteger el PAN (número de cuenta principal), que incluye el proveedor, el tipo de sistema/proceso y los algoritmos de cifrado (si corresponde), y verifique que el PAN (número de cuenta principal) quede ilegible usando uno de los siguientes métodos: • Valores hash de una vía en criptografía sólida • Truncamiento • *Token* y ensambladores de índices (los ensambladores se deben almacenar de manera segura). • Criptografía sólida con procesos y procedimientos de administración de claves asociados.	Todos los PAN guardados en un almacenamiento principal (bases de datos o archivos planos como archivos de texto y hojas de cálculo) y en almacenamiento secundario (copia de seguridad, registros de auditoría, registros de excepciones o soluciones de problemas) deben estar protegidos. Las funciones hash de una vía basadas en criptografía sólida se pueden utilizar para convertir los datos del titular de la tarjeta en ilegibles. Las funciones hash son apropiadas cuando no existe necesidad de recuperar el número original (las funciones hash de una vía son irreversibles). Se recomienda, aunque no es un requisito actual, agregar un valor de entrada aleatorio adicional a los datos del titular de la tarjeta antes de usar el hash para reducir la posibilidad de que un atacante compare los datos (y obtenga el PAN de estos) con las tablas de los valores hash computados previamente. El objetivo del truncamiento es eliminar permanentemente un segmento de los datos del PAN de modo que solo se almacene una parte (sin exceder los primeros seis y los últimos cuatro
	3.4.b Evalúe varias tablas o archivos de la muestra de repositorios de datos para controlar que el PAN (número de cuenta principal) sea ilegible (es decir, no esté almacenado en formato de texto claro).	
	3.4.c Evalúe una muestra de medios extraíbles (como copias de seguridad en cintas) para confirmar que el PAN (número de cuenta principal) sea ilegible.	
	3.4.d Revise una muestra de los registros de auditoría, incluidos los registros de la aplicación de pago, para confirmar que el PAN es ilegible o que no está presente en los registros.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.	**3.4.e** Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.	dígitos) del PAN. Un *token* de índice es un *token* criptográfico que reemplaza el PAN (número de cuenta principal) basándose en un índice determinado por un valor impredecible. Un ensamblador único es un sistema en el que una clave privada generada aleatoriamente solo se utiliza una única vez para cifrar un mensaje, que luego se descifra utilizando un ensamblador y una clave únicos que coincidan. El objetivo de una criptografía sólida (según se define en el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS*) es que el cifrado se base en un algoritmo probado y aceptado por la industria (no, en un algoritmo de propiedad exclusiva ni desarrollado internamente), con claves criptográficas sólidas. Al correlacionar las versiones en valores hash o truncadas de un PAN determinado, una persona malintencionada puede derivar fácilmente el valor original del PAN. La aplicación de controles que ayuden a prevenir la correlación de estos datos ayudará a asegurar que el PAN original permanezca ilegible.
3.4.1 Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con cuentas de usuarios.	**3.4.1.a** Si se utiliza el cifrado de disco, inspeccione la configuración y observe el proceso de autenticación a fin de verificar que el acceso lógico a los sistemas de archivos cifrados se implemente por medio de un mecanismo separado del mecanismo de autenticación del sistema operativo nativo (por ejemplo, sin utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). **3.4.1.b** Observe los procesos y entreviste al personal para verificar que las claves criptográficas se almacenen de forma segura (por ejemplo, se almacenan en medios extraíbles protegidos adecuadamente con controles de acceso seguros).	El objetivo de este requisito es abordar la aceptabilidad del cifrado de disco para lograr que los datos del titular de la tarjeta sean ilegibles. El cifrado de disco cifra todo el disco o todas las particiones que se encuentran en una computadora y descifra, automáticamente, la información cuando la solicita un usuario autorizado. Muchas soluciones de cifrado de discos interceptan las operaciones de lectura y escritura del sistema operativo y efectúan las transformaciones de cifrado apropiadas sin que el usuario realice una acción especial, salvo suministrar una contraseña al inicio de la sesión o del sistema. Según estas características de

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
Nota: *Este requisito se aplica adicionalmente a todos los demás requisitos de cifrado y de gestión de claves de la PCI DSS.*	**3.4.1.c** Revise las configuraciones y observe los procesos a fin de verificar que los datos del titular de la tarjeta almacenados en medios extraíbles se cifren en cualquier lugar donde se almacenen. ***Nota:*** *Si no se utiliza el cifrado de disco para cifrar medios extraíbles, los datos almacenados en estos medios deberán convertirse en ilegibles mediante algún otro método.*	cifrado de discos, a fin de cumplir con este requisito, el método no puede realizar lo siguiente: 1) Usar el mismo autenticador de cuentas de usuarios como sistema operativo. 2) Usar una clave de descifrado que esté asociada a las bases de datos de cuentas de usuarios locales del sistema ni a credenciales generales de inicio de sesión de la red o que derive de estas. El cifrado de disco completo ayuda a proteger los datos en caso de la pérdida física del disco y, por lo tanto, debe ser compatible con dispositivos portátiles que almacenan los datos del titular de la tarjeta.
3.5 Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido: ***Nota:*** *Este requisito también rige las claves utilizadas para cifrar datos de titulares de tarjetas almacenados y para las claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos; dichas claves de cifrado de claves deben ser al menos tan seguras como las claves de cifrado de datos.*	**3.5** Revise las políticas y los procedimientos de administración de claves y verifique que se hayan especificado los procesos que protegen las claves utilizadas para cifrar los datos del titular de la tarjeta contra su divulgación o uso indebido y deben incluir, al menos, lo siguiente: • El acceso a las claves se restringe a la menor cantidad de custodios necesarios. • Las claves de cifrado de claves deben ser, al menos, tan sólidas como las claves de cifrado de datos que protegen. • Las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos. • Las claves se almacenan de forma segura en la menor cantidad de ubicaciones y formas posibles.	Las claves de cifrado deben tener una sólida protección debido a que aquellos que obtiene acceso podrán descifrar datos. Las claves criptográficas, si se utilizan, deben ser, al menos, tan sólidas como las claves de cifrado de datos a fin de brindar la protección adecuada de la clave que cifra los datos así como de los datos cifrados con esa clave. El requisito de proteger las claves de divulgación y uso indebido se aplica tanto a claves de cifrado de datos como a claves de cifrado de claves. Debido a una clave de cifrado de claves puede otorgar acceso a muchas claves de cifrado de datos, las claves de cifrado de claves requieren medidas de protección sólidas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.5.1 ***Requisitos adicionales solo para los proveedores de servicios:*** Mantenga una descripción documentada de la arquitectura criptográfica que incluye: • Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad • Descripción del uso de la clave para cada tecla • Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves	**3.5.1** Entreviste al personal responsable y revise la documentación para verificar que existe un documento para describir la arquitectura criptográfica, que incluye: • Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad • Descripción del uso de la clave para cada tecla • Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Mantener la documentación actual de la arquitectura criptográfica permite a una entidad entender los algoritmos, los protocolos, y las claves criptográficas utilizadas para proteger los datos del titular de la tarjeta, así como los dispositivos que generan, utilizan y protegen las claves. Esto permite a una entidad seguir el ritmo de las amenazas en evolución a su arquitectura, lo que las habilita para planificar actualizaciones a medida que cambian los niveles de seguridad proporcionados por los diferentes algoritmos/complejidad de las claves. El mantenimiento de dicha documentación también permite a una entidad detectar las claves o los dispositivos de gestión de claves perdidos o faltantes, e identificar las adiciones no autorizadas a su arquitectura criptográfica.
3.5.2 Restrinja el acceso a las claves criptográficas a la menor cantidad de custodios necesarios.	**3.5.2** Revise las listas de acceso de usuarios para controlar que el acceso a las claves se restrinja a la menor cantidad de custodios necesarios.	Muy pocas personas deben tener acceso a las claves criptográficas, usualmente solo aquellos con responsabilidades de custodios de claves (esto reduce la posibilidad de que los datos del titular de la tarjeta queden visible para personas no autorizadas).

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.5.3 Siempre guarde las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. • Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). • Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria. ***Nota:*** *No es necesario guardar las claves públicas de esta manera.*	**3.5.3.a** Revise los procedimientos documentados para verificar que las claves criptográficas utilizadas para cifrar/descifrar los datos del titular de la tarjeta estén siempre en una (o más) de las siguientes formas en todo momento: • Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. • Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). • Como claves o componentes de la clave de acuerdo con los métodos aceptados por la industria.	Las claves criptográficas se deben almacenar de manera segura para evitar el acceso no autorizado o innecesario que pueda dejar expuestos los datos del titular de la tarjeta. El objetivo no es cifrar las claves de cifrado de claves; sin embargo, esas claves deben estar protegidas contra la divulgación y el uso indebido, según lo definido en el Requisito 3.5. Si se usan claves de cifrado de claves, almacenarlas en ubicaciones físicas o lógicamente separadas de las claves de cifrado de datos reduce el riesgo de acceso no autorizado a ambas claves.
	3.5.3.b Revise las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar que las claves criptográficas utilizadas para cifrar/descifrar los datos del titular de la tarjeta estén siempre en una (o más) de las siguientes formas en todo momento: • Cifrados con una clave de cifrado de claves. • Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). • Como claves o componentes de la clave de acuerdo con los métodos aceptados por la industria.	
	3.5.3.c Siempre que se usen claves de cifrado de claves, revise las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar lo siguiente: • Las claves de cifrado de claves deben ser, al menos, tan sólidas como las claves de cifrado de datos que protegen. • Las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
3.5.4 Guarde las claves criptográficas en la menor cantidad de ubicaciones posibles.	**3.5.4** Revise las ubicaciones de almacenamiento de claves y observe los procesos para verificar que las claves estén almacenadas en la menor cantidad de ubicaciones posibles.	Almacenar las claves criptográficas en la menor cantidad de ubicaciones posibles ayuda a la organización a llevar un registro y a controlar todas las ubicaciones de claves; y minimiza la posibilidad de que las claves queden expuestas a personas no autorizadas.
3.6 Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta, incluso 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** ***Procedimientos de pruebas adicionales solo para las evaluaciones de los proveedores de servicios:*** Si el proveedor de servicios comparte claves con sus clientes para la transmisión o el almacenamiento de datos del titular de la tarjeta, revise la documentación que el proveedor de servicios le proporciona a los clientes y verifique que incluya lineamientos sobre la manera de transmitir, almacenar y actualizar, de manera segura, sus claves, de conformidad con los Requisitos 3.6.1 a 3.6.8 que siguen a continuación. **3.6.b** Revise los procesos y procedimientos de administración de claves utilizados para cifrar los datos del titular de la tarjeta y realice lo siguiente:	La manera en la cual se administran las claves de cifrado es una parte crítica de la continuidad de seguridad de la solución de cifrado. Un buen proceso de administración de claves, ya sea manual o automático, como parte del producto de cifrado, se basa en las normas de la industria y abarca todos los elementos clave en 3.6.1 hasta 3.6.8. Instruir a los clientes sobre cómo transmitir, almacenar y actualizar claves criptográficas de manera segura ayuda a evitar la divulgación o el uso indebido de las claves a entidades no autorizadas. Este requisito rige para las claves utilizadas para cifrar los datos del titular de la tarjeta almacenados y cualquier clave de cifrado de claves respectiva. ***Nota:*** *Se aclaró que el Procedimiento de prueba 3.6.a solo aplica si la entidad que se evalúa es un proveedor de servicios.*
3.6.1 Generación de claves de cifrado sólido	**3.6.1.a** Verifique que los procedimientos de administración de claves especifiquen cómo generar claves sólidas. **3.6.1.b** Observe los procedimientos de generación de claves para verificar que se hayan generado claves sólidas.	La solución de cifrado debe generar claves sólidas, de acuerdo con lo definido en el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y de las PA-DSS* en “Generación de claves criptográficas”. Usar claves criptográficas sólidas aumenta el nivel de seguridad de los datos del titular de la tarjeta cifrados.
3.6.2 Distribución segura de claves de cifrado	**3.6.2.a** Verifique que los procedimientos de administración de claves especifiquen cómo distribuir las claves de manera segura.	La solución de cifrado debe distribuir las claves de forma segura, lo que significa que las claves solo se entregan a los custodios identificados en

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	3.6.2.b Observe el método de distribución de claves para verificar que se distribuyan de manera segura.	el Requisito 3.5.2 y nunca se distribuyen en el cifrado.
3.6.3 Almacenamiento seguro de claves de cifrado	**3.6.3.a** Verifique que los procedimientos de administración de claves especifiquen cómo almacenar claves de manera segura. **3.6.3.b** Observe el método de almacenamiento de claves y verifique que se almacenen de manera segura.	La solución de cifrado debe almacenar claves de forma segura, por ejemplo, cifrarlas con una clave de cifrado de claves. Almacenar claves sin la protección correcta puede provocar el acceso de atacantes, que descifrarán y visualizarán los datos del titular de la tarjeta.
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).	**3.6.4.a** Verifique que los procedimientos de administración de claves incluyan un período de cifrado definido para cada tipo de clave utilizada y que definan un proceso para los cambios de clave al finalizar el período de cifrado especificado. **3.6.4.b** Entreviste al personal para verificar que se hayan cambiado las claves al finalizar el período de cifrado.	Un período de cifrado es el intervalo durante el cual una clave criptográfica particular se puede utilizar para su propósito definido. Las consideraciones para definir el período de cifrado incluyen, pero sin limitarse a, la solidez del algoritmo subyacente, tamaño o longitud de la clave, peligro de riesgo de la clave y la confidencialidad de los datos cifrados. Es imperativo cambiar periódicamente las claves de cifrado cuando han llegado al final de su período de cifrado a fin de minimizar el riesgo de que alguien obtenga las claves de cifrado y las use para descifrar datos.
3.6.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción 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 de cifrado retiradas o reemplazadas, éstas se deben archivar de forma segura (por ejemplo, utilizando una clave de cifrado de*	**3.6.5.a** Verifique que los procedimientos de administración de claves especifiquen procesos para realizar lo siguiente: • Retiro o reemplazo de claves cuando se haya debilitado la integridad de la clave. • Reemplazo de claves que se sepa o se sospeche que estén en riesgo. • Las claves que se guardan después de retirarlas o reemplazarlas no se usan para operaciones de cifrado. **3.6.5.b** Entreviste al personal y verifique que hayan implementado los siguientes procesos: • Las claves se retiran o reemplazan cuando se ha debilitado la integridad de la clave, incluso cuando	Las claves que ya no se utilicen o necesiten, o las claves que se sepa o se sospeche que estén en riesgo, se deben anular o destruir para asegurarse de que ya no se puedan utilizar. Si es necesario guardar esas claves (por ejemplo, para respaldar datos cifrados archivados), deben tener una protección segura. La solución de cifrado debe proporcionar y facilitar un proceso para reemplazar las claves que deben ser reemplazadas o aquellas que se sepa o se sospeche que estén en riesgo.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
claves). Las claves criptográficas archivadas se deben utilizar solo con fines de descifrado o verificación.	alguien que conoce la clave deja de trabajar en la empresa. • Las claves se reemplazan si se sabe o se sospecha que están en riesgo. • Las claves que se guardan después de retirarlas o reemplazarlas no se usan para operaciones de cifrado.	
3.6.6 Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido. ***Nota:*** *Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.*	**3.6.6.a** Verifique que los procedimientos manuales de administración de claves de texto claro especifiquen procesos para realizar lo siguiente: • Conocimiento dividido de claves, de manera tal que los componentes de las claves queden bajo control de, al menos, dos personas que solo tengan conocimiento de su propio componente de la clave. • Control doble de claves, de manera tal que se necesiten, al menos, dos personas para realizar las operaciones de administración de claves y que ninguna tenga acceso al material de autenticación del otro (por ejemplo, contraseñas o claves).	El conocimiento dividido y control doble de claves se utiliza para eliminar la posibilidad de que una persona tenga acceso a toda la clave. Este control se implementa en las operaciones manuales de administración de claves o donde la administración de claves no haya sido implementada por el producto de cifrado. El conocimiento parcial es un método en el que dos o más personas tienen componentes individuales de la clave y cada persona conoce su propio componente, pero individualmente no pueden cifrar la clave criptográfica original. El control dual requiere de dos o más personas para realizar una función, y ninguna de las personas puede usar el material de autenticación de otra ni acceder a este.
	3.6.6 b Entreviste al personal y observe los procesos para verificar que las claves manuales de texto claro se administran con lo siguiente: • Conocimiento dividido. • Control doble.	
3.6.7 Prevención de sustitución no autorizada de claves criptográficas.	**3.6.7.a** Verifique que los procedimientos de administración de claves especifiquen los procesos para evitar la sustitución no autorizada de claves.	La solución de cifrado no debe permitir ni aceptar la sustitución de claves por parte de fuentes no autorizadas o procesos inesperados.
	3.6.7.b Entreviste al personal y observe los procesos para verificar que se evita la sustitución no autorizada de claves.	
3.6.8 Requisito para que los custodios de claves criptográficas declaren, formalmente, que comprenden y aceptan su responsabilidad como custodios de claves.	**3.6.8.a** Verifique que los procedimientos de administración de claves especifiquen los procesos para solicitar que los custodios de claves declaren (por escrito o electrónicamente) que comprenden y aceptan sus responsabilidades como custodios de claves.	Este proceso garantizará que los individuos que actúan como custodios de claves se comprometan con el rol de custodios de claves y que comprenden y aceptan las responsabilidades.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	3.6.8.b Observe la documentación y otra evidencia que demuestre que los custodios de claves declararon, por escrito o electrónicamente, que comprenden y aceptan sus responsabilidades como custodios de claves.	
3.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**3.7** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos documentados para administrar, de manera segura, el almacenamiento continuo de los datos del titular de la tarjeta.

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

La información confidencial se debe cifrar 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 la PCI DSS	Procedimientos de prueba	Guía
4.1 Utilizar criptografía sólida y protocolos de seguridad para proteger los datos del titular de la tarjeta confidenciales durante la transmisión por redes públicas abiertas, como por ejemplo, las siguientes: • Solo se aceptan claves y certificados de confianza. • El protocolo implementado solo admite configuraciones o versiones seguras. • La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. *Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes:* • *La Internet* • *Tecnologías inalámbricas, incluso 802.11 y Bluetooth* • *Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código)* • *Servicio de radio paquete general (GPRS)* • *Comunicaciones satelitales*	**4.1.a** Identifique todas las ubicaciones donde se transmiten o reciben datos del titular de la tarjeta en redes públicas abiertas. Revise las normas documentadas y compárelas con las configuraciones del sistema para verificar que se usen protocolos de seguridad y criptografía segura en todas las ubicaciones. **4.1.b** Revise las políticas y los procedimientos documentados para verificar que se hayan especificado los procesos para las siguientes opciones: • Para aceptar solo claves o certificados de confianza. • Para que el protocolo en uso solo acepte versiones y configuraciones seguras (que no se admitan versiones ni configuraciones inseguras). • Para implementar la solidez de cifrado correcta para la metodología de cifrado que se utiliza. **4.1.c** Seleccione y observe una muestra de las transmisiones de entrada y salida a medida que ocurren (por ejemplo, observar los procesos del sistema o el tráfico de la red) para verificar que todos los datos del titular de la tarjeta se cifran con un método de criptografía sólida durante la transmisión. **4.1.d** Revise las claves y los certificados para verificar que solo se acepten claves o certificados de confianza. **4.1.e** Evalúe las configuraciones del sistema y verifique que el protocolo implementado solo use configuraciones seguras y que no admita versiones ni configuraciones inseguras.	La información confidencial debe estar cifrada durante la transmisión en redes públicas, porque es fácil y común para una persona malintencionada interceptar y/o desviar datos mientras están en tránsito. Para transmitir los datos del titular de la tarjeta de manera segura, es necesario usar claves/certificados de confianza, protocolos de transmisión seguros y una solidez de cifrado correcta para cifrar estos datos. No se deben aceptar solicitudes de conexión de sistemas que no admiten la solidez de cifrado necesaria y que pueden generar una conexión insegura. Tenga en cuenta que algunas implementaciones de protocolos (como SSL, y SSH versión 1.0 y TLS temprana) tienen vulnerabilidades conocidas que un atacante puede utilizar para controlar el sistema afectado. Sea cual sea el protocolo de seguridad que se utiliza, asegúrese de que esté configurado para utilizar solo versiones y configuraciones seguras para evitar el uso de una conexión insegura, por ejemplo, al utilizar solo certificados de confianza única y soportar solo el cifrado sólido (no soportar protocolos o métodos más débiles e inseguros). Verificar que los certificados sean de confianza (por ejemplo, que no se hayan vencido o que los haya emitido una fuente de confianza) contribuye a garantizar la integridad de una conexión segura.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	4.1.f Evalúe las configuraciones del sistema y verifique que se implemente la solidez de cifrado correcta para la metodología de cifrado en uso. (Consulte las recomendaciones/mejores prácticas de los proveedores).	
	4.1.g Para las implementaciones de TLS, revise las configuraciones del sistema y verifique que se habilite TLS al transmitir o recibir los datos del titular de la tarjeta. Por ejemplo, para implementaciones basadas en explorador web: • "HTTPS" aparece como el protocolo URL (*Universal Record Locator)*. • Los datos del titular de la tarjeta solo se solicitan si "HTTPS" aparece como parte del URL.	Generalmente, el URL de la página web debería empezar con "HTTPS" o el explorador web debería mostrar el icono de un candado en algún lugar de la ventana del explorador. Muchos proveedores de certificados TLS también proporcionan un sello de verificación muy notorio, que suele denominarse "sello de seguridad", "sello de sitio seguro" o "sello de confianza"; en este sello, se puede hacer clic para visualizar la información del sitio web. Consulte los estándares de la industria y las mejores prácticas para obtener información acerca de la criptografía sólida y los protocolos seguros (por ejemplo, NIST SP 800-52 y SP 800-57, OWASP, etc.) ***Nota:*** SSL/TLS temprana no se considera criptografía sólida y no puede utilizarse como control de seguridad, excepto por los terminales de POS POI que se pueden verificar como no susceptibles a cualquier vulnerabilidad conocida y los puntos de terminación a los que se conectan, según se define en el Anexo A2.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
4.1.1 Asegúrese de que las redes inalámbricas que transmiten los datos del titular de la tarjeta o que están conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria a fin de implementar un cifrado sólido para la transmisión y la autenticación.	**4.1.1** Identifique todas las redes inalámbricas que transmitan datos del titular de la tarjeta o que estén conectados al entorno de datos del titular de la tarjeta. Revise las normas documentadas y compárelas con los ajustes de configuración del sistema para verificar las siguientes opciones en todas las redes inalámbricas identificadas: • Se usan las mejores prácticas de la industria para implementar un cifrado sólido para la autenticación y la transmisión. • No se usa el cifrado débil (por ejemplo, WEP, SSL) como control de seguridad para la autenticación o la transmisión.	Usuarios maliciosos pueden utilizar herramientas gratis y disponibles a gran escala para espiar comunicaciones inalámbricas. El uso de criptografía sólida ayuda a limitar la divulgación de información confidencial en las redes inalámbricas. La criptografía sólida es necesaria para la autenticación y la transmisión de los datos del titular de la tarjeta a efectos de impedir que usuarios malintencionados accedan a la red inalámbrica o que utilicen las redes inalámbricas para acceder a otras redes internas o a otros datos.
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, SMS, el chat, etc.)	**4.2.a** Si se utilizan tecnologías de mensajería de usuario final para enviar los datos del titular de la tarjeta, evalúe los procesos de envío del PAN (número de cuenta principal), revise la muestra de las transmisiones salientes a medida que ocurren y verifique que el PAN (número de cuenta principal) quede ilegible o que esté protegido mediante criptografía sólida cuando se lo envía a través de tecnologías de mensajería de usuario final.	El correo electrónico, la mensajería instantánea, SMS y el chat se pueden interceptar fácilmente con detectores de paquetes durante la entrega en redes internas y públicas. No utilice estas herramientas de mensajería para enviar el PAN (número de cuenta principal), a menos que estén configurados con un cifrado sólido. Además, si una entidad solicita PAN a través de tecnologías de mensajería de usuario final, la entidad deberá proporcionar una herramienta o método para proteger estos PAN utilizando criptografía sólida o convierta los PAN en ilegibles antes de la transmisión.
	4.2.b Revise las políticas escritas y verifique que exista una política que establezca que los PNA (número de cuenta principal) no protegidos no se deben enviar por medio de tecnologías de mensajería de usuario final.	
4.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**4.3** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para administrar, de manera segura, la transmisión continua de los datos del titular de la tarjeta.

Mantener un programa de administración de vulnerabilidad

Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.

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. Se puede considerar la opción de incluir otras soluciones antimalware como complemento del software antivirus; no obstante, estas soluciones adicionales no reemplazan la implementación del software antivirus.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven 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.	Los ataques que usan vulnerabilidades ampliamente publicadas se los denomina comúnmente “día cero” (un ataque que se aprovecha de las vulnerabilidades previamente desconocidas) y atacan a sistemas que, de lo contrario, serían seguros. Sin una solución de antivirus que se actualice regularmente, estas nuevas formas de software malicioso pueden atacar sistemas, inhabilitar una red o poner en riesgo los datos.
5.1.1 Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.	**5.1.1** Revise la documentación del proveedor y examine las configuraciones del antivirus para verificar que los programas de antivirus realicen lo siguiente: • Detecten todos los tipos conocidos de software maliciosos. • Eliminen todos los tipos de software maliciosos conocidos. • Protejan el sistema contra todos los tipos de software maliciosos conocidos. *Entre los ejemplos de tipos de software maliciosos, se pueden incluir virus, troyanos, gusanos, spyware, adware y rootkits.*	Es importante proveer protección contra **TODOS** los tipos y formas de software malicioso.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
5.1.2 Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que pueden aparecer a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.	**5.1.2** Entreviste al personal para verificar que se supervisan y evalúan las amenazas de malware en aquellos sistemas que no suelen verse afectados por software maliciosos a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.	Generalmente, los sistemas mainframe, las computadoras de alcance medio (como las AS/400) y sistemas similares no suelen verse afectados por malware. Sin embargo, las tendencias de la industria de los software maliciosos cambia rápidamente; por esta razón, es importante que las organizaciones conozcan cuáles son los nuevos malwares que podrían atacar sus sistemas, por ejemplo, mediante una supervisión de los avisos de seguridad y de los nuevos grupos de antivirus del proveedor para determinar si los sistemas podrían estar en riesgo debido a malware nuevos o futuros. Las tendencias en software maliciosos se deben incluir en la identificación de nuevas vulnerabilidades de seguridad, y los métodos para tratar nuevas tendencias se deben incorporar en las normas de configuración y los mecanismos de protección de la empresa, según sea necesario.
5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: • Estén actualizados. • Ejecuten análisis periódicos. • Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.	**5.2.a** Revise las políticas y los procedimientos para verificar que las definiciones y el software antivirus exijan actualizaciones.	Incluso las mejores soluciones de antivirus no son tan eficaces si no se realiza un mantenimiento o si no están al día con las últimas actualizaciones de seguridad, archivos de firmas o protección contra malware. Los registros de auditoría proporcionan la capacidad de supervisar actividad de virus y reacciones antimalware. Por lo tanto, es imprescindible configurar las soluciones antimalware de manera tal que generen registros de auditoría y que esos registros se administren de conformidad con el Requisito 10.
	5.2.b Revise las configuraciones de antivirus, incluso la instalación maestra del software, para verificar lo siguiente en los mecanismos de antivirus: • Estén configurados para realizar actualizaciones automáticas. • Estén configurados para realizar análisis periódicos.	
	5.2.c Revise una muestra de los componentes del sistema, incluso todos los tipos de sistemas operativos comúnmente afectados por software malicioso, a fin de controlar lo siguiente: • Las definiciones y el software antivirus estén actualizados. • Se realicen análisis periódicos.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	5.2.d Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar lo siguiente: • La generación de registro de software antivirus esté habilitada. • Los registros se conserven de acuerdo con el Requisito 10.7 de las PCI DSS.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado. ***Nota:*** *Las soluciones antivirus pueden desactivarse temporalmente, pero solo si existe una necesidad técnica legítima autorizada por la gerencia con un criterio casuístico. Si es necesario desactivar la protección antivirus por un motivo específico, debe contarse con una autorización formal. Podría ser necesario implementar medidas de seguridad adicionales para el período en que no esté activa la protección antivirus.*	**5.3.a** Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar que el software antivirus funcione activamente. **5.3.b** Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar que los usuarios no puedan deshabilitar ni modificar el software antivirus. **5.3.c** Entreviste al personal responsable y evalúe los procesos para verificar que los usuarios no puedan deshabilitar ni modificar el software antivirus, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado.	Los antivirus que funcionan constantemente y que no se pueden modificar protegen de manera continua contra malware. Implementar controles basados en políticas en todos los sistemas para evitar que se pueda modificar o deshabilitar la protección contra malware ayuda a evitar que los software maliciosos saquen provecho de las debilidades del sistema. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus, por ejemplo, desconectar de Internet el sistema sin protección mientras no haya protección de antivirus y realizar un análisis completo después de habilitarla nuevamente.
5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**5.4** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos que protegen el sistema contra malware cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para asegurarse de que los sistemas estén protegidos contra malware de manera continua.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades pueden subsanarse mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas deben contar con los parches de software correctos para evitar que personas malintencionadas o software maliciosos usen, de manera indebida, o pongan en riesgo los datos del titular de la tarjeta.

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 la PCI DSS	Procedimientos de prueba	Guía
6.1 Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, “alto”, “medio” o “bajo”) a las vulnerabilidades de seguridad recientemente descubiertas. ***Nota:*** *Las clasificaciones de riesgo deben basarse en las mejores prácticas de la industria y en la posible incidencia. Por ejemplo, los criterios para clasificar vulnerabilidades pueden incluir la puntuación base del CVSS, la clasificación del proveedor o el tipo de sistema afectado.* *Los métodos para evaluar las vulnerabilidades y asignar las clasificaciones de riesgo varían según el entorno y la estrategia de evaluación de riesgos de la organización. Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de “alto riesgo” para el entorno. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar “críticas” si suponen una amenaza inminente para el entorno, si afectan los sistemas o si generan un posible riesgo si no se contemplan. Algunos ejemplos de sistemas críticos son los*	**6.1.a** Revise las políticas y los procedimientos y verifique que los procesos estén definidos para realizar lo siguiente: • Identificar nuevas vulnerabilidades de seguridad. • Asignar una clasificación de riesgo a las vulnerabilidades en la que se identifiquen todas las vulnerabilidades de “alto riesgo” y “críticas”. • Usar fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad. **6.1.b** Entreviste al personal y observe el proceso para verificar lo siguiente: • Se identifiquen nuevas vulnerabilidades de seguridad. • Se asigne una clasificación de riesgo a las vulnerabilidades que identifique todas las vulnerabilidades de “alto riesgo” y “críticas”. • Los procesos que identifican las nuevas vulnerabilidades de seguridad incluyen usar fuentes externas conocidas para obtener información sobre vulnerabilidades de seguridad.	El objetivo de este requisito consiste en que las organizaciones conozcan cuáles son las nuevas vulnerabilidades que pueden afectar su entorno. Las fuentes de información de vulnerabilidades deben ser confiables y, generalmente, incluir sitios web de proveedores, nuevos grupos industriales, listas de correos o fuentes RSS. Después de que una organización identifique una vulnerabilidad que pueda afectar su entorno, deberá evaluar y clasificar el riesgo que esa vulnerabilidad supone. Por lo tanto, la organización debe tener implementado un método para evaluar las vulnerabilidades constantemente y asignar la clasificación de riesgo a esas vulnerabilidades. Esto no se puede realizar por medio de un análisis de ASV (proveedores aprobados de escaneo) ni con un análisis de vulnerabilidades internas; se requiere un proceso que controle activamente las fuentes de la industria para obtener información sobre las vulnerabilidades. Clasificar los riesgos (por ejemplo, como “alto”, “medio” o “bajo”) les permite a las organizaciones identificar, priorizar y abordar con mayor rapidez los puntos de mayor riesgo y reducir la probabilidad del aprovechamiento de las vulnerabilidades que suponen el mayor riesgo.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta.		
6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instalar los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. ***Nota:*** *Los parches de seguridad críticos deben identificarse de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1.*	**6.2.a** Revise las políticas y los procedimientos de instalación de parches de seguridad a fin de verificar que los procesos estén definidos para realizar lo siguiente: • Instalación de parches de seguridad críticos proporcionados por el proveedor dentro del mes del lanzamiento. • Instalación de todos los parches de seguridad proporcionados por el proveedor en un período coherente (por ejemplo, en un período de tres meses). **6.2.b** En el caso de una muestra de los 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 para verificar lo siguiente: • Los parches de seguridad críticos correspondientes proporcionados por el proveedor se instalen dentro del mes del lanzamiento. • Todos los parches de seguridad correspondientes proporcionados por el proveedor se instalen en un período específico (por ejemplo, en un plazo de tres meses).	Los ataques que usan vulnerabilidades ampliamente publicadas se los denomina comúnmente “día cero” (un ataque que se aprovecha de las vulnerabilidades previamente desconocidas) y atacan a sistemas que, de lo contrario, serían seguros. Si los parches más recientes no se implementan en los sistemas críticos rápidamente, una persona malintencionada puede aprovechar estas vulnerabilidades para atacar o inhabilitar el sistema o acceder a datos confidenciales. Al priorizar los parches para las infraestructuras críticas, se garantiza que los sistemas y los dispositivos de alta prioridad estén rápidamente protegidos contra las vulnerabilidades después del lanzamiento del parche. Considere priorizar la instalación de parches de manera tal que los parches de seguridad de los sistemas críticos o en riesgo se instalen en un plazo de 30 días y que los parches de menor riesgo se instalen en un plazo de 2 a 3 meses. Este requisito se aplica a los parches aplicables para todo el software instalado, incluidas las aplicaciones de pago (tanto para las que están validadas por la PA-DSS como las que no).
6.3 Desarrolle aplicaciones de software internas y externas (incluso acceso administrativo a aplicaciones basado en web) de manera segura y de la siguiente manera: • De acuerdo con las PCI DSS (por ejemplo, autenticación y registros	**6.3.a** Revise los procesos de desarrollo de software escritos para verificar que se basen en las normas o en las mejores prácticas de la industria. **6.3.b** Revise los procesos de desarrollo de software escritos y verifique que se incluya la seguridad de la información durante todo el ciclo de vida.	Si no se incluye la seguridad durante la definición de requisitos, el diseño, el análisis y las fases de prueba de desarrollo del software, se pueden introducir vulnerabilidades de seguridad en el entorno de producción de forma inadvertida o malintencionada.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
seguros). • Basadas en las normas o en las mejores prácticas de la industria. • Incorporación de seguridad de la información durante todo el ciclo de vida del desarrollo del software. ***Nota**: Esto rige para todos los software desarrollados internamente y para todos los software personalizados desarrollados externamente.*	**6.3.c** Evalúe los procesos de desarrollo de software escritos y verifique que las aplicaciones de software se desarrollen de conformidad con las PCI DSS. **6.3.d** Entreviste a los desarrolladores de software para verificar que se implementen los procesos de desarrollo de software escritos.	Entender cómo se administran los datos confidenciales en la aplicación, incluso cuándo se almacenan y transmiten y cuándo están en la memoria, ayuda a identificar qué áreas de datos necesitan protección.
6.3.1 Elimine las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes.	**6.3.1** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable a fin de verificar que la producción previa y las cuentas de aplicaciones personalizadas, las ID de usuarios y las contraseñas se eliminen antes de enviar la aplicación a producción o ponerla a disposición de los clientes.	Las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas se deben eliminar del código de producción antes de que la aplicación se active o se ponga a disposición de los clientes, ya que estos elementos pueden revelar información sobre el funcionamiento de la aplicación. La posesión de esa información podría facilitar que se ponga en riesgo la aplicación y los datos relacionados del titular de la tarjeta.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.3.2 Revise el código personalizado antes de enviarlo a producción o de ponerlo a disposición de los clientes a fin de identificar posibles vulnerabilidades en la codificación (mediante procesos manuales o automáticos) y que incluya, al menos, lo siguiente: • La revisión de los cambios en los códigos está a cargo de personas que no hayan creado el código y que tengan conocimiento de técnicas de revisión de código y prácticas de codificación segura. • Las revisiones de los códigos deben garantizar que el código se desarrolle de acuerdo con las directrices de codificación segura. • Las correcciones pertinentes se implementan antes del lanzamiento. • La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. *(continúa en la página siguiente)*	**6.3.2.a** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable para verificar que todos los cambios de código de las aplicaciones personalizadas (ya sea mediante procesos manuales o automáticos) se revisen de la siguiente manera: • Individuos que no sean el autor que originó el código e individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura revisan los cambios en los códigos. • Las revisiones de los códigos 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.	Las vulnerabilidades de personalidad en códigos personalizados suelen ser blanco de personas malintencionadas para obtener acceso a una red y poner en riesgo los datos de titulares de tarjetas. Aquellas personas que tengan conocimientos en técnicas de revisión de código y en prácticas de codificación segura deben participar en el proceso de revisión. La revisión de los códigos debe estar a cargo de personas que no hayan creado el código para que se realice de forma objetiva e independiente. También se pueden usar procesos o herramientas automáticos en lugar de realizar revisiones manuales, pero recuerde que puede ser difícil, o incluso imposible, que la herramienta automática identifique algunos problemas de codificación. Corregir los errores de codificación antes de implementar el código en el entorno de producción o antes de que se les envíe a los clientes impide que el código exponga los entornos a un posible uso indebido. Es mucho más difícil y costoso corregir un código defectuoso después de implementarlo o si se envió a los entornos de producción. Incluir la revisión formal y la aprobación final de la gerencia antes del envío garantiza que el código está aprobado y que se ha desarrollado de acuerdo con las políticas y los procedimientos.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 a los efectos de tratar las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.*	**6.3.2.b** Seleccione una muestra de los cambios recientes de las aplicaciones personalizadas y verifique que los códigos de aplicaciones personalizadas se revisen de acuerdo con el punto 6.3.2.a mencionado 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** Revise las políticas y los procedimientos y verifique que se define lo siguiente: • Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control de acceso para reforzar la separación. • Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y el personal asignado al entorno de producción. • Los datos de producción (PAN activos) no se usan en las pruebas ni en el desarrollo. • Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción. • Se documentan los procedimientos de control de cambios relacionados con la implementación de parches de seguridad y las modificaciones del software.	Si los controles de cambio no se documentan ni implementan correctamente, las funciones de seguridad se pueden omitir o dejar inoperables por error o deliberadamente, pueden ocurrir irregularidades de procesamiento o se puede introducir un código malicioso.
6.4.1 Separe los entornos de desarrollo/prueba de los entornos de producción y refuerce la separación con controles de acceso.	**6.4.1.a** Revise la documentación de la red y la configuración de los dispositivos de red a fin de verificar que los entornos de desarrollo/prueba estén separados de los entornos de producción.	Debido al estado constantemente cambiante de los entornos de desarrollo y prueba, estos tienden a ser menos seguros que el entorno de producción. Sin una separación correcta entre los entornos, es posible que el entorno de producción y los datos del titular de la tarjeta queden en riesgo debido a la configuración de seguridad menos estricta y a las vulnerabilidades en un entorno de prueba o desarrollo.
	6.4.1.b Revise la configuración de los controles de acceso y verifique que se implementen estos controles para reforzar la separación entre los entornos de desarrollo/prueba y los entornos de producción.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción	**6.4.2** Observe los procesos y entreviste al personal asignado a los entornos de desarrollo/prueba y al personal asignado al entorno de producción para verificar que se implementen las tareas de separación entre los entornos de desarrollo/prueba y el de producción.	Reducir el número de personal con acceso al entorno de producción y a los datos de titulares de tarjeta minimiza el riesgo y ayuda a asegurar que ese acceso se limite a aquellos individuos con una necesidad de conocimiento de la empresa. El objetivo de este requisito consiste en separar las funciones de desarrollo y prueba de las funciones de producción. Por ejemplo, un desarrollador puede utilizar una cuenta a nivel del administrador con privilegios elevados en el entorno de desarrollo, y tener una cuenta separada con acceso a nivel de usuario al entorno de producción.
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo	**6.4.3.a** Observe los procesos de pruebas y entreviste al personal para verificar que se implementen los procedimientos a fin de garantizar que los datos de producción (PAN activos) no se usen en las pruebas ni en el desarrollo.	Los controles de seguridad no suelen ser tan estrictos en el entorno de prueba o desarrollo. El uso de datos de producción proporciona a personas malintencionadas la oportunidad de obtener acceso no autorizado a estos datos (datos de los titulares de tarjetas).
	6.4.3.b Revise una muestra de datos de pruebas para verificar que los datos de producción (PAN activos) no se utilicen en las pruebas ni en el desarrollo.	
6.4.4 Eliminación de datos y cuentas de los componentes del sistema antes de que se activen los sistemas de producción	**6.4.4.a** Observe los procesos de pruebas y entreviste al personal para verificar que las cuentas y los datos de pruebas se eliminen antes de activar el sistema de producción.	Los datos y las cuentas de prueba se deben eliminar del código de producción antes de activar los componentes del sistema, ya que estos elementos pueden revelar información sobre el funcionamiento de la aplicación o del sistema. Contar con dicha información podría dar lugar a que se ponga en riesgo el sistema y los datos del titular de la tarjeta relacionados.
	6.4.4.b Revise una muestra de los datos y las cuentas del sistema de producción recientemente instalado o actualizado para verificar que los datos y las cuentas se eliminen antes de activar el sistema.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.4.5 Los procedimientos de control de cambios deben incluir lo siguiente:	**6.4.5.a** Revise los procedimientos de control de cambios documentados y verifique que los procedimientos estén definidos según lo siguiente: • Documentación de incidencia • Aprobación de cambio documentada por las partes autorizadas. • Pruebas de funcionalidad a fin de verificar que el cambio no impacta negativamente en la seguridad del sistema. • Procedimientos de desinstalación	Si no se administra adecuadamente, es posible que el impacto de las actualizaciones del software y de los parches de seguridad no se perciba completamente y podría ocasionar consecuencias inesperadas.
	6.4.5.b En el caso de una muestra de componentes del sistema, entreviste al personal responsable para determinar los cambios recientes. Realice un seguimiento de los cambios relacionados con la documentación de control de cambios. Por cada cambio que evalúe, realice lo siguiente:	
6.4.5.1 Documentación de incidencia.	**6.4.5.1** Verifique que la documentación de incidencia se incluya en la documentación del control de cambios de cada muestra de cambio.	Se debe documentar el impacto del cambio para que todas las partes afectadas puedan programar, de manera apropiada, cualquier cambio de procesamiento.
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.	**6.4.5.2** Verifique que la aprobación documentada por las partes autorizadas esté presente para cada muestra de cambio.	La aprobación de las partes autorizadas indica que el cambio es legítimo y está autorizado por la organización.
6.4.5.3 Verifique que se hayan realizado las pruebas de funcionalidad y que el cambio no impacte negativamente en la seguridad del sistema.	**6.4.5.3.a** En el caso de las muestras de cambio, revise que las pruebas de funcionalidad se hayan realizado para verificar que el cambio no impacte negativamente en la seguridad del sistema.	Se deben realizar pruebas rigurosas para verificar que la seguridad del entorno no se reduce al implementar un cambio. Las pruebas deben validar que todos los controles de seguridad existentes permanecen implementados, que se reemplacen por controles igualmente sólidos o que se refuercen después de realizar un cambio en el entorno.
	6.4.5.3.b En el caso de los 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 en producción.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.4.5.4 Procedimientos de desinstalación.	**6.4.5.4** Verifique que se preparen los procedimientos de desinstalación para cada muestra de cambio.	Para cada cambio, se deben documentar los procedimientos de desinstalación en caso de que el cambio falle o afecte negativamente la seguridad de la aplicación o del sistema y para permitir que el sistema vuelva al estado previo.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.4.6 Al término de un cambio significativo, deben implementarse todos los requisitos pertinentes de la PCI DSS en todos los sistemas y redes nuevos o modificados, y la documentación actualizada según sea el caso.	**6.4.6** Para una muestra de los cambios significativos, revise los registros de cambios, entreviste al personal, y observe los sistemas/redes afectados para verificar que se implementaron los requisitos aplicables de la PCI DSS y que se actualizó la documentación como parte del cambio.	Tener procesos para analizar cambios significativos ayuda a garantizar que todos los controles apropiados de la PCI DSS se aplican a cualquier sistema o red agregado o modificado dentro del entorno en el alcance. La construcción de esta validación en los procesos de gestión de cambio ayuda a garantizar que los inventarios de los dispositivos y las normas de configuración se mantienen actualizados y los controles de seguridad se aplican donde sea necesario. Un proceso de gestión de cambio deberá incluir evidencia de apoyo que los requisitos de la PCI DSS se implementan o preservan mediante el proceso iterativo. Ejemplos de los requisitos de la PCI DSS que se verían afectados incluyen, pero no se limitan a: • El Diagrama de una red se actualiza para reflejar los cambios. • Los sistemas están configurados según las normas de configuración, con todas las contraseñas predeterminadas cambiadas y los servicios innecesarios deshabilitados. • Los sistemas están protegidos con los controles requeridos, por ejemplo, la supervisión de la integridad de archivos (FIM), los antivirus, los parches, y el registro de auditoría. • Los datos confidenciales de autenticación (SAD) no se almacenan y todo el almacenamiento de los datos del titular de la tarjeta (CHD) se documenta e incorpora en las políticas y procedimientos de retención de datos • Los nuevos sistemas se incluyen en el proceso trimestral de análisis de vulnerabilidad.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.5 Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo de software de la siguiente manera: • Capacite a los desarrolladores, por lo menos anualmente, en las técnicas actualizadas de codificación segura, incluida la forma de evitar las vulnerabilidades de codificación comunes. • Desarrollar aplicaciones basadas en directrices de codificación seguras. ***Nota:*** *Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.10 eran congruentes con las mejores prácticas de la industria al momento de la publicación de esta versión de la 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.a** Revise las políticas y los procedimientos de desarrollo de software y verifique que a los desarrolladores se les exija una capacitación actualizada en técnicas de codificación segura, según las guías y las mejores prácticas de la industria. **6.5.b** Revise los registros de capacitación para verificar que los desarrolladores de software hayan sido capacitados en técnicas de codificación segura por lo menos anualmente, en las que se incluya cómo evitar las vulnerabilidades de codificación comunes. **6.5.c** Verifique que los procesos implementados protejan las aplicaciones, al menos, contra las siguientes vulnerabilidades:	La capa de aplicación es de alto riesgo y puede ser el blanco de amenazas internas y externas. Los Requisitos 6.5.1 al 6.5.10 hacen referencia a los controles mínimos que se deben implementar, y las organizaciones deben incorporar prácticas de codificación segura relevantes que correspondan a la tecnología particular de su entorno. Los desarrolladores de la aplicación deben estar debidamente capacitados para identificar y solucionar los problemas relacionados con estas (y otras) vulnerabilidades de codificación comunes. Contar con personal que tenga conocimientos en directrices de codificación segura minimizará la cantidad de vulnerabilidades de seguridad introducidas mediante prácticas de codificación poco seguras. La capacitación de los desarrolladores puede estar a cargo de personal de la empresa o de terceros y debe ser pertinente a la tecnología utilizada. A medida que cambian las prácticas de codificación segura aceptadas por la industria, las prácticas de codificación de las organizaciones y la capacitación de los desarrolladores se deben actualizar para abordar nuevas amenazas, por ejemplo, ataques para extraer la memoria. Las vulnerabilidades identificadas en los Requisitos 6.5.1 al 6.5.10 proporcionan un punto de partida mínimo. Es responsabilidad de la organización informarse sobre las últimas tendencias en vulnerabilidades e incorporar las medidas apropiadas en cuanto a las prácticas de codificación segura.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
Nota: *Los Requisitos 6.5.1 al 6.5.6, que se describen a continuación, rigen para todas las aplicaciones de pago (internas o externas).*		
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** Evalúe las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden los errores de inyección y realicen lo siguiente: • Validación de la entrada para comprobar que los datos de los usuarios no puedan modificar el significado de los comandos ni de las consultas. • Uso de consultas basadas en parámetros.	Los errores de inyección, en especial, los errores de inyección SQL, son métodos comúnmente utilizados para poner en riesgo aplicaciones. La inyección se produce cuando se envían datos suministrados por el usuario a un intérprete como parte de un comando o una consulta. Los datos hostiles del atacante engañan al intérprete para que ejecute comandos accidentales o cambie datos, y le permiten atacar los componentes que hay dentro de la red a través de la aplicación para iniciar ataques, como desbordamientos de buffer, o para revelar información confidencial y la funcionalidad de la aplicación del servidor. La información se debe validar antes de enviarse a la aplicación; por ejemplo, mediante la verificación de todos los caracteres alfabéticos, la combinación de caracteres numéricos y alfabéticos, etc.
6.5.2 Desbordamiento de buffer	**6.5.2** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden los desbordamientos de buffer y realicen lo siguiente: • Validación de los límites del buffer. • Truncamiento de cadenas de entrada.	Los desbordamientos de buffer ocurren cuando una aplicación no tiene los límites necesarios para verificar su espacio de buffer. Esto puede ocasionar la información en el buffer se expulse del espacio de memoria del buffer y que entre en el espacio de memoria ejecutable. Cuando esto ocurre, el atacante puede insertar código malicioso al final del buffer y luego introducir ese código en espacio de memoria ejecutable desbordando el buffer. Luego, el código malicioso se ejecuta y, con frecuencia, permite que el atacante acceda, de manera remota, a la aplicación o al sistema infectado.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.5.3 Almacenamiento cifrado inseguro	**6.5.3** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden el almacenamiento criptográfico inseguro y realicen lo siguiente: • Prevenga errores de cifrado. • Utilice claves y algoritmos criptográficos sólidos.	Las aplicaciones que no utilizan correctamente las funciones criptográficas sólidas para almacenar datos tienen más posibilidades de estar en riesgo y de dejar expuestas las credenciales de autenticación o los datos del titular de la tarjeta. Si un atacante puede sacar provecho de los procesos criptográficos débiles, también puede obtener acceso como texto no cifrado a los datos cifrados.
6.5.4 Comunicaciones inseguras	**6.5.4** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que se aborden las comunicaciones inseguras mediante técnicas de codificación que autentique y cifren correctamente todas las comunicaciones confidenciales:	Las aplicaciones que no cifran correctamente el tráfico de red con una criptografía sólida tienen más posibilidades de estar en riesgo y de dejar expuestos los datos del titular de la tarjeta. Si un atacante puede sacar provecho de los procesos criptográficos débiles, también puede tener el control de la aplicación o, incluso, obtener acceso en texto claro a los datos cifrados.
6.5.5 Manejo inadecuado de errores	**6.5.5** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que el manejo inadecuado de errores se corrige mediante técnicas de codificación que no filtran información por medio de mensajes de error (por ejemplo, enviando detalles genéricos del error, en lugar de enviar detalles específicos).	Las aplicaciones pueden filtrar, por equivocación, información sobre su configuración o sobre los trabajos internos, o pueden exponer información privilegiada mediante métodos de manejo inadecuado de errores. Los atacantes utilizan estas debilidades para hurtar datos confidenciales o para poner en riesgo todo el sistema. Si una persona malintencionada puede crear errores que una aplicación web no puede manejar correctamente, puede obtener información detallada del sistema, puede crear interrupciones por negación de servicios, puede hacer que la seguridad falle o puede bloquear el servidor. Por ejemplo, el mensaje “la contraseña suministrada es incorrecta” le indica al atacante que la ID de usuario suministrada es correcta y que debe centrar sus esfuerzos solo en la contraseña. Utilice mensajes de error más genéricos, como “no se pueden verificar los datos”.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.5.6 Todas las vulnerabilidades de “alto riesgo” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS).	**6.5.6** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que las técnicas de codificación aborden las vulnerabilidades de “alto riesgo” que puedan afectar la aplicación, según lo especificado en el Requisito 6.1 de las PCI DSS.	Todas las vulnerabilidades identificadas en el proceso de clasificación de riesgos de vulnerabilidades de la organización (definido en el Requisito 6.1) que sean de “alto riesgo” y que puedan afectar la aplicación se deben identificar y corregir durante el desarrollo de la aplicación.
Nota: *Los Requisitos 6.5.7 al 6.5.10, que siguen a continuación, rigen para las aplicaciones web y las interfaces de las aplicaciones (internas o externas):*		Las aplicaciones web (públicas), tanto internas como externas, tienen riesgos de seguridad únicos según su arquitectura, su facilidad relativa y la ocurrencia de riesgos.
6.5.7 Lenguaje de comandos entre distintos sitios (XSS)	**6.5.7** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que el XSS (lenguaje de comandos entre distintos sitios) se aborde con las técnicas de codificación que incluyen lo siguiente: • Validación de todos los parámetros antes de la inclusión. • Uso de técnicas de escape sensibles al contexto.	Los errores de XSS (lenguaje de comandos entre distintos sitios) se producen cuando una aplicación toma datos suministrados por el usuario y los envía a un explorador web sin primero validar ni codificar ese contenido. El XSS (lenguaje de comandos entre distintos sitios) permite a los atacantes ejecutar secuencias en el explorador de la víctima, el cual puede apropiarse de las sesiones del usuario, destruir sitios web y posiblemente introducir gusanos, etc.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.5.8 Control de acceso inapropiado (como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios).	**6.5.8** Evalúe las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que el control de acceso inapropiado, como las referencias no seguras a objetos directos, la no restricción de acceso a URL y la exposición completa de los directorios, se aborde mediante técnicas de codificación que incluyan lo siguiente: • Autenticación correcta de usuarios. • Desinfección de entradas. • No exposición de referencias a objetos internos a usuarios. • Interfaces de usuarios que no permitan el acceso a funciones no autorizadas.	Una referencia a un objeto directo ocurre cuando un desarrollador expone una referencia a un objeto de implementación interna, como un archivo, directorio, registro de base de datos o clave, como un parámetro de URL o formulario. Los atacantes pueden manipular esas referencias para acceder a otros objetos sin autorización. Refuerce constantemente el control de acceso en la capa de presentación y la lógica de negocios para todas las URL. Con frecuencia, la única manera en que una aplicación protege funciones confidenciales es evitando que se muestren vínculos o URL a usuarios no autorizados. Los atacantes pueden usar esta debilidad para tener acceso y realizar operaciones no autorizadas mediante el acceso a esos URL directamente. Es posible que un atacante enumere y explore la estructura del directorio de un sitio web (exposición completa de los directorios) y así obtener acceso a información no autorizada, así como un mayor conocimiento de los trabajos del sitio para posterior explotación. Si las interfaces de usuarios permitan el acceso a funciones no autorizadas, es posible que personas no autorizadas accedan a credenciales con privilegios o a los datos del titular de la tarjeta. Solo aquellos usuarios autorizados deberían tener permiso para acceder a referencias de objetos directos desde recursos confidenciales. Limitar el acceso a los recursos de datos ayudará a evitar que recursos no autorizados accedan a los datos del titular de la tarjeta.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF)	**6.5.9** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que, para corregir la CSRF (falsificación de solicitudes entre distintos sitios), se utilicen técnicas de codificación que aseguren que las aplicaciones no confían en las credenciales de autorización ni en los *tokens* que los exploradores presentan automáticamente.	Ante un ataque de CSRF (falsificación de solicitudes entre distintos sitios), el explorador de la víctima que inició sesión debe enviar una solicitud previamente autenticada a una aplicación web vulnerable, lo que le permite al atacante realizar operaciones de cambio de estado que la víctima está autorizada a realizar (por ejemplo, actualizar los detalles de la cuenta, realizar compras o, incluso, autenticar la aplicación).
6.5.10 Autenticación y administración de sesión interrumpidas.	**6.5.10** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que la autenticación y la administración de sesión interrumpidas se aborden con técnicas de codificación que, generalmente, incluyen lo siguiente: • Marcas de *tokens* de sesión (por ejemplo, cookies) como “seguros”. • No exposición de las ID de la sesión en el URL. • Incorporación de tiempos de espera apropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente.	La autenticación y la administración de sesión seguras impiden que personas malintencionadas pongan en riesgo credenciales, claves o *tokens* de sesión de cuentas legítimas que podrían permitir que un intruso adopte la identidad de un usuario autorizado.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 con 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 ***Nota:*** *Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2.* • Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, *firewall* de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.	**6.6** En el caso de aplicaciones web *públicas*, asegúrese de que se haya implementado *alguno* de los siguientes métodos: • Evalúe los procesos documentados, entreviste al personal y examine los registros de las evaluaciones de seguridad de las aplicaciones para verificar que se hayan revisado las aplicaciones web públicas, mediante herramientas o métodos manuales o automáticos para la evaluación de la seguridad de vulnerabilidades, de la siguiente manera: – Por lo menos, anualmente – Después de cualquier cambio – Por una organización que se especialice en seguridad de aplicaciones – Al menos, todas las vulnerabilidades del Requisito 6.5 se incluyan en la evaluación – Que se corrijan todas las vulnerabilidades – La aplicación se vuelva a analizar después de las correcciones • Revise los parámetros de la configuración del sistema y entreviste al personal responsable para verificar que se haya implementado una solución técnica automática que detecte y prevenga ataques web (por ejemplo, un *firewall* de aplicación web) de la siguiente manera: – Se encuentre delante de las aplicaciones web públicas para detectar y prevenir ataques web. – Funcione activamente y esté actualizada, según corresponda. – Genere registros de auditoría. – Esté configurada para bloquear ataques web o para generar una alerta que se investiga de inmediato.	Las aplicaciones web públicas son los principales blancos de los atacantes y las aplicaciones web con códigos deficientes permiten que los atacantes accedan, fácilmente, a los datos confidenciales y a los sistemas. El objetivo del requisito de revisar las aplicaciones o de instalar *firewalls* en las aplicaciones web es reducir la cantidad de riesgos que enfrentan las aplicaciones web públicas debido a las prácticas de administración de aplicaciones o de codificación deficientes. • Se utilizan herramientas o métodos de evaluación de seguridad de vulnerabilidad, tanto manuales como automáticos, para revisar o probar las aplicaciones a fin de determinar si existen vulnerabilidades. • Los *firewalls* de aplicación web filtran y bloquean el tránsito no esencial en la capa de aplicación. Junto con un *firewall* de red, un *firewall* de aplicación web correctamente configurado previene ataques a la capa de aplicación si las aplicaciones están codificadas o configuradas incorrectamente. Esto se puede lograr a través de una combinación de tecnología y proceso. Las soluciones basadas en procesos deben tener mecanismos que faciliten respuestas oportunas a las alertas con el fin de cumplir con la intención de este requisito, que es prevenir los ataques. ***Nota:*** *"La organización que se especializa en seguridad de aplicación" puede ser una tercera empresa o una organización interna, siempre que los revisores se especialicen en seguridad de aplicaciones y puedan demostrar independencia respecto del equipo de desarrollo.*

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
6.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**6.7** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar las políticas de seguridad y los procedimientos operativos para asegurarse de que los sistemas se desarrollen de manera segura y que estén protegidos contra vulnerabilidades de manera continua.

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 que tenga la empresa

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

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

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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.	**7.1** Revise las políticas escritas para el control de acceso y verifique que incorporen los Requisitos 7.1.1 al 7.1.4 de la siguiente manera: • Definición de las necesidades de acceso y asignación de privilegios de cada función. • Restricción de acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo. • Asignación de acceso según la tarea, la clasificación y la función de cada persona. • Aprobación documentada (por escrito o electrónicamente) de las partes autorizadas para todos los accesos, que incluye la lista de los privilegios específicos aprobados.	Mientras más gente tenga acceso a los datos de titulares de tarjetas, más riesgo hay de que una cuenta de usuario se use maliciosamente. Limitar el acceso a quienes tienen una razón de negocios legítima para tener acceso ayuda a la organización a prevenir el manejo incorrecto de los datos del titular de la tarjeta por falta de experiencia o por maldad.
7.1.1 Defina las necesidades de acceso de cada función, incluso lo siguiente: • Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. • Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	**7.1.1** Seleccione una muestra de funciones y verifique que las necesidades de acceso de cada función estén definidas e incluyan lo siguiente: • Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. • Identificación de los privilegios necesarios de cada función para que puedan desempeñar sus funciones.	A fin de limitar el acceso a los datos del titular de la tarjeta exclusivamente a las personas que necesiten acceder, primero se deben definir las necesidades de acceso de cada función (por ejemplo, administrador del sistema, personal del centro de llamados, empleado de la tienda), los sistemas/dispositivos/datos de acceso que necesita cada función y el nivel de privilegio necesario para que las funciones puedan realizar las tareas asignadas. Después de definir las funciones y las necesidades de acceso correspondientes, se podrá otorgar el permiso de acceso correspondiente a cada función. *(continúa en la página siguiente)*

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
7.1.2 Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.	**7.1.2.a** Entreviste al personal responsable de asignar los accesos para verificar que el acceso de usuarios con ID privilegiadas cumple con lo siguiente: • Se asigna solamente a las funciones que específicamente necesitan acceso privilegiado. • Estén restringidos a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.	Cuando se asignan ID privilegiadas, es importante asignar solo los privilegios necesarios para realizar el trabajo (la "menor cantidad de privilegios"). Por ejemplo, el administrador de la base de datos o el administrador de copias de seguridad no deben tener los mismos privilegios asignados como administrador general del sistema.
	7.1.2.b Seleccione una muestra de las ID de usuarios con acceso privilegiado y entreviste al personal de administración responsable a fin de verificar que los privilegios asignados respeten lo siguiente: • Sean necesarios para el trabajo de la persona. • Estén restringidos a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.	Asignar la menor cantidad de privilegios evita que los usuarios que no tengan el conocimiento suficiente de la aplicación cambien, de manera incorrecta o por accidente, la configuración de la aplicación o alteren los parámetros de seguridad. Asignar la menor cantidad de privilegios también ayuda a reducir el alcance del daño si una persona no autorizada accede a la ID del usuario.
7.1.3 Asigne el acceso según la tarea, la clasificación y la función del personal.	**7.1.3** Seleccione una muestra de las ID de usuarios y entreviste al personal de administración responsable para verificar que los privilegios se asignen según la clasificación y la función laboral de la persona.	Después de definir los roles del usuario (de conformidad con el Requisito 7.1.1 de las PCI DSS), resulta sencillo otorgar acceso a los usuarios según su clasificación y función laboral con los roles ya creados.
7.1.4 Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.	**7.1.4** Seleccione una muestra de las ID de usuario y compárelas con la aprobación documentada para verificar lo siguiente: • Exista una aprobación documentada para los privilegios asignados. • Las partes autorizadas realizaron la aprobación. • Los privilegios especificados coinciden con los roles asignados a la persona.	La aprobación documentada (por ejemplo, por escrito o electrónicamente) garantiza que la gerencia conoce y autoriza a aquellas personas a quienes se les otorgaron accesos y privilegios, y que necesitan el acceso para realizar su trabajo.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según 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 parámetros del sistema y la documentación del proveedor para verificar que el sistema de control de acceso se implemente de la siguiente manera:	Sin un mecanismo para restringir el acceso en base a la necesidad de conocer que tiene el usuario, es posible que sin saberlo se le otorgue acceso a los datos de titulares de tarjetas a un usuario. El sistema de control de acceso automatiza el proceso para restringir accesos y asignar privilegios. Además, una configuración predeterminada de “negar todos” garantiza que no se le otorgará el acceso a nadie, salvo que se establezca una regla que otorgue dicho acceso. Las entidades pueden tener uno o más sistemas de control de acceso para gestionar el acceso de los usuarios. ***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.*
7.2.1 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 una persona se basa en la clasificación del trabajo y su función.	**7.2.2** Confirme que los sistemas de control de acceso estén configurados de manera tal que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función.	
7.2.3 Configuración predeterminada de “negar todos”.	**7.2.3** Confirme que los sistemas de control de acceso cuenten con la configuración predeterminada de “negar todos”.	
7.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**7.3** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para asegurarse de que el acceso esté controlado, que se limita siempre en función de la necesidad de saber y de la menor cantidad de privilegios.

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema.

Al asignar una ID (identificación) exclusiva a cada persona que tenga acceso garantiza que cada una se hará responsable de sus actos. Cuando se ejerce dicha responsabilidad, las medidas implementadas en datos y sistemas críticos están a cargo de procesos y usuarios conocidos y autorizados y, además, se puede realizar un seguimiento.

La eficacia de una contraseña se determina, en gran medida, por el diseño y la implementación del sistema de autenticación, especialmente, la frecuencia con la que el atacante intenta obtener la contraseña y los métodos de seguridad para proteger las contraseñas de usuarios en los puntos de acceso durante la transmisión y el almacenamiento.

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. Esto incluye las cuentas que usan los proveedores y terceros (por ejemplo, para respaldo o mantenimiento). Estos requisitos no se aplican a las cuentas utilizadas por los consumidores (por ejemplo, los titulares de tarjetas).*

Sin embargo, los Requisitos del 8.1.1, 8.2, 8.5, 8.2.3 al 8.2.5, y del 8.1.6 al 8.1.8 no rigen para las cuentas de usuarios dentro de una aplicación de pago de un punto de venta que solo tenga acceso a un número de tarjeta por vez a fin de facilitar una transacción única (como las cuentas en efectivo).

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:	**8.1.a** Revise los procedimientos y confirme que definen procesos para cada uno de los siguientes puntos, desde el 8.1.1 hasta el 8.1.8.	Si una organización se asegura que cada usuario tiene una identificación única (en vez de usar una misma ID para varios empleados), puede mantener la responsabilidad individual de las acciones y una pista de auditorías efectiva por empleado. Esto resulta útil para acelerar la resolución de problemas y la contención cuando se producen usos indebidos o acciones malintencionadas.
	8.1.b Verifique que se implementen los procedimientos para la administración de identificación de usuarios mediante las siguientes acciones:	
8.1.1 Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.	**8.1.1** Entreviste al personal administrativo y confirme que todos los usuarios tengan asignada una ID exclusiva para tener acceso a los componentes del sistema o los datos del titular de la tarjeta.	
8.1.2 Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación.	**8.1.2** En el caso de una muestra de ID de usuarios privilegiados e ID de usuarios generales, evalúe las autorizaciones asociadas y observe los parámetros del sistema a fin de verificar que todas las ID de usuarios y las ID de usuarios privilegiados se hayan implementado solamente con los privilegios especificados en la aprobación documentada.	Para asegurarse de que las cuentas de usuarios que tengan acceso a los sistemas sean usuarios válidos y reconocidos, los procesos sólidos deben administrar todos los cambios de las ID de usuarios y otras credenciales de autenticación, incluso, la incorporación de credenciales nuevas y la modificación o eliminación de credenciales existentes.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.1.3 Cancele de inmediato el acceso a cualquier usuario cesante.	**8.1.3.a** Seleccione una muestra de los usuarios cesantes en los últimos seis meses y revise las listas de acceso de usuarios actuales, tanto para acceso local como remoto, para verificar que sus ID se hayan desactivado o eliminado de las listas de acceso.	Si un empleado se va de la empresa y aún tiene acceso a la red con su cuenta de usuario, se puede producir un acceso innecesario o malintencionado a los datos del titular de la tarjeta, ya sea por parte del exempleado o por parte de un usuario malintencionado que saque ventaja de la cuenta anterior y sin uso. Para prevenir el acceso no autorizado, se deben cancelar rápidamente (lo antes posible) las credenciales del usuario y otros métodos de autenticación cuando el empleado deja la empresa.
	8.1.3.b Verifique que todos los métodos de autenticación físicos, como tarjetas inteligentes, *tokens*, etc., se hayan devuelto o desactivado.	
8.1.4 Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.	**8.1.4** Observe las cuentas de usuarios y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.	Generalmente, las cuentas que no se usan regularmente son blancos de ataques, ya que es poco probable que se note algún cambio (como el cambio de la contraseña). Por lo tanto, es más fácil que se aprovechen de estas cuentas y las utilicen para acceder a los datos del titular de la tarjeta.
8.1.5 Administre las ID que usan los terceros para acceder, respaldar o mantener los componentes del sistema de manera remota de la siguiente manera: • Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. • Se deben monitorear mientras se usan.	**8.1.5.a** Entreviste al personal y observe los procesos de administración de cuentas que usan los proveedores para acceder, respaldar o mantener los componentes del sistema a fin de verificar que las cuentas que usan los proveedores para acceder de manera remota cumplen con lo siguiente: • Se inhabilitan cuando no se usan. • Se habilitan solo cuando el proveedor las necesita y se deshabilitan cuando no se usan.	Si permite que los proveedores tengan acceso a su red las 24 horas del día, los 7 días de la semana en caso de que necesiten realizar el mantenimiento de sus sistemas, aumentarán las posibilidades de acceso no autorizado, ya sea por parte de un usuario del entorno del proveedor o de una persona malintencionada que encuentra y usa este punto de acceso externo a la red siempre disponible. Habilitar el acceso solamente durante el período que sea necesario y deshabilitarlo cuando ya no sea necesario previene el uso indebido de estas conexiones. Monitorear el acceso del proveedor sirve para garantizar que los proveedores acceden solo a los sistemas necesarios y en los momentos autorizados.
	8.1.5.b Entreviste al personal y observe los procesos para verificar que se monitoreen las cuentas de acceso remoto de los terceros mientras se utilizan.	
8.1.6 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.	**8.1.6.a** En el caso de una muestra de componentes del sistema, 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 realizar, como	Sin la implementación de mecanismos de bloqueo de cuentas, un atacante puede intentar adivinar continuamente una contraseña a través de herramientas manuales o automatizadas (por ejemplo, el craqueo de contraseñas), hasta lograr

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	máximo, seis intentos de inicio de sesión no válidos.	su objetivo y obtener acceso a la cuenta de un usuario. ***Nota:*** *Se aclaró que el Procedimiento de prueba 8.1.6.b solo aplica si la entidad que se evalúa es un proveedor de servicios.*
	8.1.6.b *Procedimientos de pruebas adicionales para los proveedores de servicios*: Revise los procesos internos y la documentación de cliente/usuario y observe los procesos implementados para verificar que las cuentas de usuarios no consumidores se bloqueen de forma temporal después de, como máximo, seis intentos no válidos de acceso.	
8.1.7 Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.	**8.1.7** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que solicite que, al bloquear la cuenta de un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.	Si se bloquea una cuenta debido a que una persona ha estado intentando adivinar una contraseña de manera insistente, los controles para retrasar la reactivación de estas cuentas bloqueadas evitan que la persona malintencionada siga adivinando la contraseña (tendrá que detenerse durante un mínimo de 30 minutos hasta que se reactive la contraseña). Además, si es necesario solicitar la reactivación, el administrador o la mesa de ayuda pueden validar que es el propietario de la cuenta quien solicita la reactivación.
8.1.8 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente.	**8.1.8** En el caso de una muestra de componentes del sistema, 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.	Cuando los usuarios se alejan de una máquina abierta que tiene acceso a componentes críticos del sistema o a los datos del titular de la tarjeta, es posible que otras personas utilicen la máquina durante la ausencia del usuario, lo que generaría el acceso no autorizado a la cuenta o un uso indebido. La reautenticación se puede aplicar en el nivel de sistema para proteger todas las sesiones que estén en ejecución en la máquina o en el nivel de la aplicación.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar 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 exclusiva y una autenticación adicional (por ejemplo, una contraseña/frase) para acceder a los datos del titular de la tarjeta, realice lo siguiente: • Revise la documentación que describe los métodos de autenticación utilizados. • Para cada tipo de método de autenticación utilizado y para cada tipo de componente del sistema, observe una autenticación para verificar que funcione de forma coherente con los métodos de autenticación documentado.	Estos métodos de autenticación, cuando se usan además de las ID exclusivas, ayudan a impedir que las ID de los usuarios corran riesgos, ya que quien intenta poner en peligro la cuenta necesita saber la ID exclusiva y la contraseña (u otro elemento de autenticación). Tenga en cuenta que un certificado digital es una opción válida para “algo que el usuario tenga” siempre que sea exclusivo para ese usuario en particular. Uno de los primeros pasos que realizará una persona malintencionada para poner en riesgo un sistema es aprovechar las contraseñas débiles o no existentes; por eso, es importante implementar buenos procesos para la administración de la autenticación.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.2.1 Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida.	**8.2.1.a** Evalúe la documentación del proveedor y los parámetros de configuración del sistema para verificar que las contraseñas se protegen durante la transmisión y el almacenamiento mediante una criptografía sólida.	Muchos de los dispositivos y aplicaciones de la red transmiten contraseñas legibles y sin cifrar a través de la red o almacenan contraseñas sin cifrado. Una persona malintencionada puede interceptar, fácilmente, contraseñas no cifradas durante la transmisión utilizando un "sniffer", o puede acceder directamente a las contraseñas no cifradas en los archivos en que estén almacenadas y utilizar estos datos para obtener acceso no autorizado. ***Nota:*** *Los procedimientos de pruebas 8.2.1.d y 8.2.1.e son procedimientos adicionales que solo se aplican si la entidad que se está evaluando es un proveedor de servicios.*
	8.2.1.b En el caso de una muestra de componentes del sistema, revise los archivos de las contraseñas para verificar que sean ilegibles durante el almacenamiento.	
	8.2.1.c En el caso de una muestra de los componentes del sistema, revise la transmisión de datos para verificar que las contraseñas sean ilegibles durante la transmisión.	
	8.2.1.d ***Procedimientos de pruebas adicionales para los proveedores de servicios:*** Observe los archivos de contraseñas y verifique que las contraseñas de los clientes sean ilegibles durante el almacenamiento.	
	8.2.1.e ***Procedimientos de pruebas adicionales solo para los proveedores de servicios:*** Observe los archivos de contraseñas y verifique que las contraseñas de los clientes no consumidores sean ilegibles durante la transmisión.	
8.2.2 Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos *tokens* o genere nuevas claves.	**8.2.2** Revise los procedimientos de autenticación para modificar las credenciales de autenticación y observe al personal de seguridad a fin de verificar que, si un usuario solicita el restablecimiento de una credencial de autenticación por teléfono, correo electrónico, Internet u otro método no personal, la identidad del usuario se verificará antes de modificar la credencial de autenticación.	Muchas personas malintencionadas usan la "ingeniería social" (por ejemplo, llaman a una mesa de ayuda y se hacen pasar por usuarios legítimos) para cambiar la contraseña y poder utilizar una ID de usuario. Considere usar una "pregunta secreta" que solo el usuario correcto pueda responder para ayudar a los administradores a identificar el usuario antes de restablecer o modificar las credenciales de autenticación.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.2.3 Las contraseñas/frases deben tener lo siguiente: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.	**8.2.3.a** En el caso de una muestra de los componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de la contraseña del usuario se encuentren configurados de manera que soliciten, al menos, la siguiente solidez o complejidad: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos. **8.2.3.b** ***Procedimientos de pruebas adicionales para los proveedores de servicios:*** Revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de usuarios no consumidores cumplan, al menos, con la siguiente solidez o complejidad: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	Las contraseñas/frases sólidas constituyen la primera línea de defensa de una red, ya que personas malintencionadas con frecuencia intentarán buscar cuentas sin contraseñas o cuyas contraseñas sean débiles. Si las contraseñas son cortas o fáciles de adivinar, será relativamente fácil para una persona malintencionada encontrar estas cuentas débiles y poner en riesgo una red utilizando una ID de usuario válida. Este requisito especifica que las contraseñas/frases deben tener un mínimo de siete caracteres numéricos y alfabéticos. Si no puede alcanzar la longitud mínima de caracteres debido a limitaciones técnicas, las entidades pueden utilizar parámetros de "solidez equivalente" para evaluar sus alternativas. Para obtener información sobre la variabilidad y la complejidad de la contraseña (también conocida como entropía) para las contraseñas/frases de seguridad de diferentes formatos, consulte los estándares de la industria (por ejemplo, la versión actual de NIST SP 800-63.) ***Nota:*** *Se aclaró que el Procedimiento de prueba 8.2.3.b solo aplica si la entidad que se evalúa es un proveedor de servicios.*
8.2.4 Cambie la contraseña/frase de usuario, al menos, cada 90 días.	**8.2.4.a** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña, al menos, cada 90 días. **8.2.4.b** ***Procedimientos de pruebas adicionales solo para los proveedores de servicios:*** *Revise los procesos internos* y la documentación del cliente/usuario y verifique lo siguiente: • Las contraseñas de usuarios no consumidores se deben cambiar periódicamente; y • Se debe orientar a los usuarios no consumidores sobre cuándo y en qué situaciones deben cambiar las	Las contraseñas/frases que se mantienen vigentes durante largos períodos sin cambiarlas proporcionan a las personas malintencionadas más tiempo para descubrirlas. ***Nota:*** *Se aclaró que el Procedimiento de prueba 8.2.4.b solo aplica si la entidad que se evalúa es un proveedor de servicios.*

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	contraseñas.	
8.2.5 No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas.	**8.2.5.a** Para una 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 para que soliciten que las nuevas contraseñas no sean iguales a las últimas cuatro contraseñas utilizadas.	Si no se conserva el historial de contraseñas, la efectividad del cambio de contraseñas es menor, dado que se puede volver a utilizar una contraseña anterior una y otra vez. Esta medida de no volver a utilizar las contraseñas durante cierto período reduce la posibilidad de que, en el futuro, se utilicen contraseñas que ya hayan sido descifradas o forzadas. ***Nota:*** *Se aclaró que el Procedimiento de prueba 8.2.5.b solo aplica si la entidad que se evalúa es un proveedor de servicios.*
	8.2.5.b ***Procedimientos de pruebas adicionales para los proveedores de servicios:*** Revise los procesos internos y la documentación de cliente/usuario para verificar que las nuevas contraseñas de usuarios no consumidores no puedan ser iguales a las últimas cuatro contraseñas utilizadas anteriormente.	
8.2.6 Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso.	**8.2.6** Revise 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.	Si se usa la misma contraseña para cada usuario nuevo, un usuario interno, un exempleado o una persona malintencionada pueden saber o descubrir fácilmente esta contraseña y usarla para obtener acceso a cuentas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.3 Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores. ***Nota:*** *La autenticación de múltiples factores requiere que se utilicen un mínimo de 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 múltiples factores.*		La autenticación de múltiples factores exige que una persona presente un mínimo de dos formas separadas de autenticación (como se describe en el Requisito 8.2), antes de otorgarse acceso. La autenticación de múltiples factores proporciona la certeza adicional de que la persona que intenta acceder es quien dice ser. Con la autenticación de múltiples factores, un atacante tendría que comprometer al menos dos mecanismos de autenticación diferentes, lo que aumenta la dificultad de riesgo, y de esa manera reducirlo. La autenticación de múltiples factores no se requiere, tanto en el nivel de sistema y en el nivel de aplicación para un componente del sistema en particular. La autenticación de múltiples factores puede realizarse, ya sea tras la autenticación para la red en particular o para el componente del sistema. Ejemplos de tecnologías de múltiples factores incluyen, entre otros, autenticación remota y RADIUS (servicio dial-in) con *tokens*; TACACS (sistema de control de acceso mediante control del acceso desde terminales) con *tokens*; y otras tecnologías que faciliten la autenticación de múltiples factores.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.3.1 Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo.	**8.3.1.a** Revise las configuraciones de la red y/o sistema, según sea el caso, para verificar que la autenticación de múltiples factores se requiere para todo el acceso administrativo que no es de consola en el CDE.	Este requisito está destinado a aplicarse a todo el personal con acceso administrativo al CDE. Este requisito se aplica solo al personal con acceso administrativo y solo para el acceso que no sea de consola para el CDE; no se aplica a las cuentas de la aplicación o de los sistemas que realizan funciones automatizadas. Si la entidad no utiliza la segmentación para separar el CDE del resto de su red, un administrador podría utilizar la autenticación de múltiples factores, ya sea al iniciar sesión en la red del CDE o al iniciar sesión en un sistema. Si el CDE está segmentado del resto de la red de la entidad, un administrador tendría que utilizar la autenticación de múltiples factores al conectarse a un sistema de CDE desde una red que no es del CDE. La autenticación de múltiples factores puede ser implementada a nivel de red o a nivel de sistema/aplicación; no tiene que ser ambos. Si el administrador utiliza MFA al iniciar sesión en la red del CDE, tampoco necesitan utilizar la MFA para iniciar sesión en un sistema o aplicación en particular en el CDE.
	8.3.1.b Observe un grupo de empleados (por ejemplo, usuarios y administradores) que se conectan de manera remota al CDE y verifique que se usen, al menos, dos de los tres métodos de autenticación.	
8.3.2 Incorpore la autenticación de múltiples factores para todo acceso remoto que se origine desde fuera de la red de la entidad (tanto para usuarios como administradores, e incluso para todos los terceros involucrados en el soporte o mantenimiento).	**8.3.2.a** Revise la configuración del sistema para los servidores y sistemas de acceso remoto, y verifique que se exija la autenticación de múltiples factores en los siguientes casos: • Todo el acceso remoto por parte del personal, tanto del usuario como del administrador, y • Acceso remoto de todos los terceros/proveedores (incluye el acceso a aplicaciones y componentes del sistema para soporte o mantenimiento).	El objetivo de este requisito es aplicarlo a todo el personal, incluso usuarios generales, administradores y proveedores (para soporte o mantenimiento) que tengan acceso remoto a la red, en los casos en que dicho acceso remoto podría otorgar acceso al CDE. Si el acceso remoto se realiza en la red de una entidad que tiene una segmentación apropiada, de modo tal que los usuarios remotos no pueden acceder al entorno de datos del titular de la tarjeta ni afectarlo, no es necesaria la autenticación de múltiples factores para el acceso remoto a esa red. Sin embargo, la autenticación de múltiples factores se requiere para cualquier acceso remoto a redes con acceso al entorno de datos del titular de la tarjeta, y se recomienda para todos los accesos remotos a las
	8.3.2.b Observe una muestra de empleados (por ejemplo, usuarios y administradores) que se conectan de manera remota a la red y verifique que se usen, al menos, dos de los tres métodos de autenticación.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
		redes de una entidad.
8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios, que incluye lo siguiente: • Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para no seleccionar contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.	**8.4.a** Revise los procedimientos y entreviste al personal para verificar que los procedimientos y las políticas de autenticación se distribuyen a todos los usuarios.	Comunicarles a todos los usuarios los procedimientos relacionados con las contraseñas y la autenticación ayuda a entender y cumplir las políticas. Por ejemplo, entre los lineamientos para seleccionar contraseñas sólidas, se pueden incluir sugerencias para ayudar al personal a seleccionar contraseñas difíciles de adivinar y que no tengan palabras del diccionario ni información del usuario (por ejemplo, la ID del usuario, nombre de familiares, fechas de nacimiento, etc.). Entre los lineamientos para proteger las credenciales de autenticación, se puede incluir no escribir las contraseñas ni guardarlas en archivos no seguros y estar atentos a personas malintencionadas que intenten hurtar sus contraseñas (por ejemplo, llamar a un empleado y solicitar su contraseña para poder “solucionar el problema”). Instruir a los usuarios para que cambien la contraseña si existe la posibilidad de que esta deje de ser segura puede prevenir que usuarios malintencionados utilicen una contraseña legítima para obtener acceso no autorizado.
	8.4.b Revise los procedimientos y las políticas de autenticación que se le entregan a los usuarios y verifique que incluyan lo siguiente: • Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para los usuarios para que no seleccionen contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.	
	8.4.c Entreviste a un grupo de usuarios y verifique que conozcan los procedimientos y las políticas de autenticación.	
8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: • Las ID de usuario genéricas se deben desactivar o eliminar. • 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.a** En el caso de una muestra de los componentes del sistema, revise las listas de ID de usuarios y verifique lo siguiente: • Las ID de usuario genéricas se deben desactivar o eliminar. • 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.	Si varios usuarios comparten las mismas credenciales de autenticación (por ejemplo, cuenta de usuario y contraseña), resulta imposible realizar un seguimiento del acceso al sistema y de las actividades de cada persona. Esto, a su vez, evita que una entidad se responsabilice por las acciones de una persona o que tenga un inicio de sesión eficaz, ya que cualquier persona del grupo que conozca las credenciales de autenticación puede haber realizado la acción.
	8.5.b Revise las políticas y los procedimientos de autenticación y verifique que el uso de ID y/o contraseñas u otros métodos de autenticación grupales y compartidos estén explícitamente prohibidos.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	8.5.c Entreviste a los administradores del sistema y verifique que las contraseñas de grupo y compartidas u otros métodos de autenticación no se distribuyan, incluso si se solicitan.	
8.5.1 ***Requisitos adicionales solo para los proveedores de servicios:*** Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente. ***Nota:*** *El objetivo de este requisito no es aplicarlo a los proveedores de servicios de hosting compartido que acceden a su propio entorno de hosting, donde se alojan numerosos entornos de clientes.*	**8.5.1** ***Procedimientos de pruebas adicionales solo para los proveedores de servicios:*** Revise las políticas y los procedimientos de autenticación y entreviste al personal para verificar que se utilicen diferentes credenciales de autenticación para acceder a cada cliente.	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Para evitar poner riesgo a varios clientes mediante el uso de un solo conjunto de credenciales, los proveedores que tienen cuentas con acceso remoto a los entornos de clientes deben utilizar una credencial de autenticación diferente para cada cliente. Las tecnologías, como los mecanismos de dos factores, que proporcionan una credencial exclusiva para cada conexión (por ejemplo, mediante una contraseña de un solo uso) también pueden cumplir con el objetivo de este requisito.
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, *tokens* de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: • Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. • Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.	**8.6.a** Revise las políticas y los procedimientos de autenticación para verificar que los procedimientos que usan mecanismos de autenticación, como *tokens* de seguridad físicos, tarjetas inteligentes y certificados, estén definidos e incluyan lo siguiente: • Los mecanismos de autenticación se asignan a una sola cuenta y no se comparten entre varias. • Los controles físicos y lógicos se definen para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.	Si varias cuentas pueden usar mecanismos de autenticación de usuarios, como *tokens*, tarjetas inteligentes y certificados, no será posible identificar quién usa el mecanismo de autenticación. Al tener controles físicos y lógicos (por ejemplo, un PIN, datos biométricos o una contraseña) para identificar, específicamente, al usuario de la cuenta se evita que usuarios no autorizados accedan usando un mecanismo de autenticación compartido.
	8.6.b Entreviste al personal de seguridad y verifique que se asignen mecanismos de autenticación a una sola cuenta y que no se compartan entre varias.	
	8.6.c Examine los parámetros de configuración del sistema y los controles físicos, según corresponda, para verificar que se implementen controles a fin de garantizar que solo la cuenta deseada usa esos mecanismos para acceder.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
8.7 Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera: • Todo acceso, consultas y acciones de usuario en las bases de datos se realizan, únicamente, mediante métodos programáticos. • Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas en estas. • Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos (no las pueden usar los usuarios ni otros procesos que no pertenezcan a la aplicación).	**8.7.a** Revise los parámetros de configuración de la aplicación y de la base de datos, y verifique que todos los usuarios estén autenticados antes de acceder.	Sin autenticación de usuario para obtener acceso a bases de datos y aplicaciones, se incrementa el potencial de acceso no autorizado o malintencionado, el cual no se puede registrar porque el usuario no se sometió a un proceso de autenticación y, por lo tanto, el sistema no puede reconocerlo. Además, solo se debe otorgar acceso a la base de datos a través de métodos programáticos (por ejemplo, a través de procedimientos almacenados) y no, a través del acceso directo a la base de datos por parte de usuarios finales (a excepción de los DBA, que pueden necesitar acceso directo a la base de datos debido a sus tareas administrativas).
	8.7.b Revise los parámetros de configuración de la base de datos y de la aplicación para verificar que el acceso de todos los usuarios, las consultas del usuario y las acciones del usuario (por ejemplo, mover, copiar, eliminar) en la base de datos se realicen únicamente mediante métodos programáticos (por ejemplo, a través de procedimientos almacenados).	
	8.7.c Evalúe los parámetros de control de acceso de la base de datos y los parámetros de configuración de la aplicación de la base de datos y verifique que el acceso directo del usuario a la base de datos, o las consultas a esta, esté limitado a los administradores de la base de datos.	
	8.7.d Revise los parámetros de control de acceso de la base de datos, los parámetros de configuración de la aplicación de la base de datos y las ID de aplicaciones relacionadas para verificar que solo las aplicaciones pueden usar las ID de la aplicación (y no los usuarios u otros procesos).	
8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**8.8** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos de identificación y autenticación cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para administrar la identificación y autorización.

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” hace referencia a todos los medios en papel y electrónicos que contienen datos del titular de la tarjeta.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.	**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 del titular de la tarjeta. • 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 datos del titular de la tarjeta y verifique que estén “aseguradas” y se impida el uso no autorizado.	Sin controles de acceso físico, como sistemas de placas y controles en las puertas, personas no autorizadas podrían obtener acceso a la instalación para robar, inhabilitar, interrumpir o destruir sistemas críticos y datos del titular de la tarjeta. Bloquear las ventanas de inicio de sesión de la consola evita que personas no autorizadas accedan a información confidencial, alteren la configuración del sistema, introduzcan vulnerabilidades en la red o destruyan registros.
9.1.1 Utilice cámaras de video u otros mecanismos de control de acceso (o ambos) para supervisar el acceso	**9.1.1.a** Verifique que las cámaras de video u otros mecanismos de control de acceso (o ambos) se usen para supervisar los puntos de entrada y salida de áreas confidenciales.	Al investigar violaciones físicas, estos controles pueden ayudar a identificar quiénes y cuándo accedieron, físicamente, a las áreas confidenciales

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 públicas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.*	**9.1.1.b** Verifique que las cámaras de video u otros mecanismos de control de acceso (o ambos) estén protegidos contra alteraciones o desactivaciones.	y cuándo salieron. Los delincuentes que intentan acceder físicamente a las áreas confidenciales, con frecuencia, intentan inhabilitar o sortear los controles de supervisión. Para evitar que se alteren estos controles, se deben colocar cámaras de video en un lugar que sea inalcanzable y que, al mismo tiempo, detecten acciones de alteración. De igual manera, se deben supervisar los mecanismos de control de acceso o instalar mecanismos de protección físicos para evitar que personas malintencionadas los dañen o deshabiliten.
	9.1.1.c Verifique que se controlen las cámaras de video u otros mecanismos de control de acceso, y que los datos de dichas cámaras o mecanismos se almacenen, al menos, durante tres meses.	Entre los ejemplos de áreas confidenciales, se incluyen las salas de servidores de la base de datos corporativa, los centros de gestión operativa en comercios minoristas que almacenan datos del titular de la tarjeta y las áreas de almacenamiento de grandes cantidades de datos del titular de la tarjeta. Cada organización debe identificar las áreas confidenciales para asegurarse de implementar los controles de supervisión físicos necesarios.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.1.2 Implemente controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público. *Por ejemplo, las conexiones de red en áreas públicas y en las que pueden acceder los visitantes se pueden inhabilitar y habilitar solo cuando el acceso a la red se autoriza explícitamente. De forma alternativa, se pueden implementar procesos para asegurarse de que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.*	**9.1.2** Entreviste al personal responsable y observe las ubicaciones de las conexiones de red de acceso público para verificar que se implementen controles físicos o lógicos a fin de restringir el acceso a las conexiones de red de acceso público.	Restringir el acceso a las conexiones de red (o a los puertos de red) impedirá que personas malintencionadas se conecten a los puertos de red disponibles y accedan a los recursos internos de la red. Independientemente de que usen controles lógicos o físicos, o ambos, debe haber la cantidad correcta para evitar que una persona o dispositivo que no esté explícitamente autorizado se conecte a la red.
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, *gateways*, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.	**9.1.3** Verifique que se restrinja correctamente el acceso físico a los puntos de acceso inalámbricos, *gateways*, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.	Sin mecanismos de seguridad para el acceso a componentes y dispositivos inalámbricos, usuarios malintencionados podrían utilizar los dispositivos inalámbricos desprovistos de seguridad de una organización para acceder a los recursos de la red o, incluso, conectar sus propios dispositivos a la red inalámbrica a fin de obtener acceso no autorizado. Además, proteger el hardware de red y comunicaciones evita que usuarios malintencionados intercepten el tráfico de la red o conecten físicamente sus propios dispositivos a los recursos de la red cableada.
9.2 Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes, de la siguiente manera: • Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). • Cambios en los requisitos de acceso. • Revocar las identificaciones de	**9.2.a** Revise los procesos documentados para verificar que los procedimientos se definan de manera tal que se pueda realizar una identificación y distinción entre empleados y visitantes. • Verifique que los procesos incluyan lo siguiente: • Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). • Cambiar los requisitos de acceso. • Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación).	Identificar a los visitantes autorizados de modo que puedan distinguirse fácilmente del personal interno evita que visitantes no autorizados obtengan acceso a áreas que contienen datos de titulares de tarjetas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación).	**9.2.b** Observe los procesos para identificar y distinguir entre empleados y visitantes, y verifique lo siguiente: • Los visitantes están claramente identificados. • Es fácil distinguir entre empleados y visitantes.	
	9.2.c Verifique que el acceso al proceso de identificación (como el sistema de placas) esté limitado solo al personal autorizado.	
9.3 Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera: • El acceso debe estar autorizado y basarse en la función de cada persona. • El acceso debe cancelarse inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, deben devolverse o desactivarse.	**9.3.a** En el caso de un grupo de empleados con acceso físico a un área confidencial, entreviste al personal responsable y observe las listas de control de acceso para verificar lo siguiente: • El acceso al área confidencial está autorizado. • La persona necesita acceder para realizar su trabajo.	Controlar el acceso físico a un área confidencial, sirve para garantizar que solo accederá el personal autorizado que tenga una necesidad empresarial legítima. Si un empleado deja de trabajar en la empresa, todos los mecanismos de acceso físico se deben devolver o inhabilitar rápidamente (lo antes posible) para garantizar que el empleado no podrá acceder, físicamente, a un área confidencial, cuando ya no trabaje más en la empresa.
	9.3.b Observe el acceso del personal a un área confidencial, para verificar que todo el personal tenga autorización antes de que accedan.	
	9.3.c Seleccione una muestra de empleados que hayan dejado de trabajar recientemente y revise las listas de control de acceso para verificar que no tenga acceso físico a un área confidencial.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.4 Implemente procedimientos para identificar y autorizar a los visitantes. Los procedimientos deben incluir lo siguiente:	**9.4** Verifique que los controles de acceso y las autorizaciones de los visitantes se implementen de la siguiente manera:	Los controles de los visitantes son importantes para reducir la posibilidad de que personas no autorizadas y malintencionadas obtengan acceso a las instalaciones (y, posiblemente, a los datos del titular de la tarjeta). Los controles de los visitantes son útiles para garantizar que estos se identifiquen como visitantes para que el personal pueda supervisar sus actividades; y que su acceso se restrinja solo a la duración de su visita legítima. Controlar la devolución de las placas de visitantes al finalizar la visita evita que personas malintencionadas usen un pase previamente autorizado para acceder, físicamente, al edificio después de finalizada la visita. Llevar un registro de visitantes que contenga un mínimo de información sobre el visitante es sencillo y económico y, además, ayuda a identificar el acceso físico a un edificio o sala y el posible acceso a los datos del titular de la tarjeta.
9.4.1 Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y estarán acompañados en todo momento.	**9.4.1.a** Observe los procedimientos y entreviste al personal para verificar que los visitantes reciben autorización antes de acceder a áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y que estén siempre acompañados.	
	9.4.1.b Observe el uso de las placas para visitantes u otro tipo de identificación a fin de verificar que las placas de identificación física no permitan el acceso sin acompañantes a áreas físicas donde se procesan o conservan datos del titular de la tarjeta.	
9.4.2 Se identifican los visitantes y se les entrega una placa u otro elemento de identificación con fecha de vencimiento y que permite diferenciar claramente entre empleados y visitantes.	**9.4.2.a** Observe las personas dentro de las instalaciones para verificar que se usen placas para visitantes u otro tipo de identificación, y que los visitantes se puedan distinguir fácilmente de los empleados que trabajan en la empresa.	
	9.4.2.b Verifique que las placas para visitantes y otro tipo de identificación tengan vencimiento.	
9.4.3 Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento.	**9.4.3** Observe la salida de los visitantes de las instalaciones para verificar que se solicite la entrega de su placa o de otro tipo de identificación al partir o al momento del vencimiento.	
9.4.4 Se usa un registro de visitantes para llevar una pista de auditoría física de la actividad de los visitantes en las instalaciones, en las salas de informática y en los centros de datos donde se almacenan o se transmiten los datos del titular de la tarjeta. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico	**9.4.4.a** Verifique que se implemente un registro de visitantes para registrar el acceso físico a las instalaciones, así como también a las salas de informática y a los centros de datos donde se almacenan o transmiten los datos del titular de la tarjeta.	
	9.4.4.b Verifique que el registro incluya lo siguiente: • Nombre del visitante • Empresa representada • Empleado que autoriza el acceso físico	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.	**9.4.4.c** Verifique que el registro se conserve durante, al menos, tres meses.	
9.5 Proteja físicamente todos los medios.	**9.5** Verifique que los procedimientos para proteger los datos del titular de la tarjeta incluyan controles para el resguardo seguro de todos los medios (entre otros, computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faxes).	El objetivo de los controles para el resguardo seguro de todos los medios es evitar que personas no autorizadas accedan a los datos del titular de la tarjeta que se encuentren en cualquier medio. Los datos de titulares de tarjetas son susceptibles de revisiones, copias o análisis no autorizados si no se protegen mientras están en medios extraíbles o portátiles, si se imprimen o se dejan sobre el escritorio de alguien.
9.5.1 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 en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.	**9.5.1** Verifique que el lugar de almacenamiento se revise una vez al año al menos para determinar que el almacenamiento de medios de copia de seguridad sea seguro.	Si el almacenamiento se realiza en un lugar no seguro, las copias de seguridad que contienen los datos del titular de la tarjeta se pueden perder, hurtar o copiar fácilmente con fines malintencionados. Revisar el lugar de almacenamiento periódicamente le permite a la organización abordar los problemas de seguridad identificados de manera oportuna y minimizar los posibles riesgos.
9.6 Lleve un control estricto de la distribución interna o externa de todos los tipos de medios y realice lo siguiente:	**9.6** Verifique que exista una política para controlar la distribución de medios y que dicha política abarque todos los medios distribuidos, incluso los que se distribuyen a personas.	Los procedimientos y los procesos ayudan a proteger los datos de titulares de tarjetas almacenados en medios que se distribuyen a usuarios internos y/o externos. Sin dichos procedimientos, los datos se pueden perder, robar y utilizarse con fines fraudulentos.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.6.1 Clasifique los medios para poder determinar la confidencialidad de los datos.	**9.6.1** Verifique que todos los medios se hayan clasificado para poder determinar la confidencialidad de los datos.	Es importante que se identifiquen los medios para poder distinguir el estado de clasificación fácilmente. Los medios no identificados como confidenciales no se pueden proteger correctamente o se pueden perder o hurtar. ***Nota:*** *Esto no significa que los medios deban tener una etiqueta con la inscripción "confidencial"; el objetivo es que la organización identifique los medios que contienen datos confidenciales para poder protegerlos.*
9.6.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.	**9.6.2.a** Entreviste al personal y revise los registros para verificar que todos los medios enviados fuera de la empresa estén registrados y se envíen por correo seguro u otro método de envío que se pueda rastrear. **9.6.2.b** Seleccione una muestra actual de varios días de registros de seguimiento externos de todos los medios y verifique que se documenten los detalles de seguimiento.	Los medios son susceptibles de pérdida o hurto si se envían a través de un método al que no se pueda hacer seguimiento, tal como un correo postal regular. Usar un servicio de correo seguro para entregar los medios que contienen datos del titular de la tarjeta les permite a las organizaciones usar su propio servicio de rastreo a fin de llevar un inventario y conocer la ubicación de los envíos.
9.6.3 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área segura (incluso, cuando se distribuyen los medios a personas).	**9.6.3** Seleccione una muestra actual de varios días de registros de seguimiento externos de todos los medios. Mediante la evaluación de los registros y las entrevistas al personal responsable, verifique que se cuente con la debida autorización de la gerencia cuando sea necesario trasladar los medios desde un área segura (incluso cuando los medios se distribuyen a personas).	Sin un proceso firme que garantice que todos los traslados de medios estén aprobados antes de retirarlos de las áreas seguras, no se podrá realizar un correcto seguimiento de los medios, ni protegerlos adecuadamente, y se desconocerá su ubicación, lo que puede generar la pérdida o robo de los medios.
9.7 Lleve un control estricto del almacenamiento y la accesibilidad de los medios.	**9.7** Obtenga y revise la política para controlar el almacenamiento y el mantenimiento de todos los medios y verifique que la política requiera inventarios periódicos de medios.	Sin métodos de inventario ni controles de almacenamiento rigurosos, el hurto o la pérdida de medios podría pasar desapercibida durante una cantidad indefinida de tiempo. Si los medios no se incluyen en un inventario, el hurto o pérdida de los mismos pudiera pasar desapercibida durante un largo período de tiempo o para siempre.
9.7.1 Lleve un registro detallado del inventario de todos los medios y lleve a cabo inventarios de los medios, al menos, una vez al año.	**9.7.1** Revise los registros de inventarios de los medios para verificar que se conserven los registros y que se lleven a cabo inventarios de medios, al menos, una vez al año.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.8 Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales de la siguiente manera:	**9.8** Revise periódicamente la política de destrucción de medios y verifique que abarque todos los medios y que defina requisitos para lo siguiente: • Los materiales de copias en papel se deben cortar en tiras, incinerarse o convertirse en pulpa para tener la certeza de que no podrán reconstruirse. • Los contenedores de almacenamiento que se usan para los materiales que se destruirán deben estar protegidos. • Los datos del titular de la tarjeta en los medios electrónicos deben quedar irrecuperables (por ejemplo, a través de un programa con la función de borrado seguro según las normas aceptadas en la industria para lograr una eliminación segura o mediante la destrucción física de los medios).	Si no se realiza un procedimiento para destruir la información contenida en discos duros, unidades portátiles, discos de CD/DVD o que se haya imprimido antes de desecharla, es posible que personas malintencionadas recuperen la información a partir de medios desechados, lo que podría crear una situación de riesgo para los datos. Por ejemplo, personas malintencionadas pueden utilizar una técnica conocida como "recolección urbana", en la que se registran contenedores de basura y papeleras de reciclaje para buscar información que se pueda utilizar para perpetrar un ataque. Proteger los contenedores de almacenamiento utilizados para los materiales que se destruirán evita que se capture información confidencial mientras se recolectan los materiales. Por ejemplo, los contenedores para los cortes en tiras pueden tener una traba para impedir el acceso a su contenido o impedir el acceso físico dentro del contenedor. Entre los ejemplos de métodos para destruir medios electrónicos de manera segura, se incluyen borrado seguro, desmagnetización o destrucción física (como desbastar o triturar discos duros).
9.8.1 Corte en tiras, incinere o convierta en pulpa los materiales de copias en papel para que no se puedan reconstruir los datos del titular de la tarjeta. Proteja los contenedores de almacenamiento destinados a los materiales que se destruirán.	**9.8.1.a** Entreviste al personal y revise los procedimientos para verificar que los materiales de copias en papel se corten en tiras, se incineren o se conviertan en pulpa para tener la certeza de que no podrán reconstruirse.	
	9.8.1.b Revise los contenedores de almacenamiento utilizados para los materiales que se destruirán y verifique que dichos contenedores estén asegurados.	
9.8.2 Controle que los datos del titular de la tarjeta guardados en medios electrónicos sean irrecuperables para que no se puedan reconstruir.	**9.8.2** Verifique que los datos del titular de la tarjeta guardados en dispositivos electrónicos sean irrecuperables (por ejemplo, a través de un programa con la función de borrado seguro según las normas aceptadas en la industria para lograr una eliminación segura o mediante la destrucción física de los medios).	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.9 Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones. ***Nota:*** *Estos requisitos rigen para los dispositivos de lectura de tarjetas que se usan en transacciones (es decir, al pasar o deslizar la tarjeta) en los puntos de venta. Este requisito no pretende regir los componentes de ingreso manual de claves, como teclados de computadoras y teclados numéricos de POS.*	**9.9** Revise las políticas y los procedimientos documentados para verificar que se realice lo siguiente: • Conservar una lista de los dispositivos. • Inspeccionar los dispositivos periódicamente para buscar intentos de alteración o sustitución. • Capacitar al personal para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos.	Los delincuentes intentan robar los datos del titular de la tarjeta mediante el hurto o la manipulación de terminales y dispositivos de lectura de tarjetas. Por ejemplo, intentan robar dispositivos para aprender cómo ingresar ilícitamente; con frecuencia, intentar reemplazar dispositivos legítimos con dispositivos fraudulentos que les envían información de la tarjeta de pago cada vez que se ingresa una tarjeta. Los delincuentes también intentan agregar componentes “de duplicado” fuera de los dispositivos; estos componentes están diseñados para capturar detalles de la tarjeta de pago, incluso, antes de que la tarjeta ingrese en el dispositivo. Por ejemplo, agregan un lector de tarjetas adicional en la parte superior del lector original, de esta manera, la información de la tarjeta de pago se captura dos veces: una con el componente del delincuente y otra con el componente legítimo del dispositivo. De esta manera, las transacciones se realizarán sin interrupciones mientras el delincuente “duplica” la información de la tarjeta de pago durante el proceso. Este requisito se recomienda para los componentes de ingreso de claves manuales, como los teclados de computadoras y teclados numéricos de POS (puntos de ventas), pero no es obligatorio. En el sitio web del PCI SSC, se encuentran disponibles otras mejores prácticas para prevenir la duplicación de datos.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.9.1 Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única	**9.9.1.a** Revise la lista de los dispositivos y verifique que incluya lo siguiente: • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única	Llevar una lista actualizada de los dispositivos le ayuda a la organización a llevar un registro de la supuesta ubicación de los dispositivos y a identificar, rápidamente, la falta o pérdida de un dispositivo. Para llevar una lista de los dispositivos, se puede utilizar un método automático (por ejemplo, un sistema de administración de dispositivos) o manual (por ejemplo, documentarlos en registros electrónicos o de papel). En el caso de los dispositivos externos, la ubicación puede incluir el nombre del empleado a quien se le asigna el dispositivo.
	9.9.1.b Seleccione una muestra de dispositivos de la lista y observe la ubicación del dispositivo para verificar que la lista sea exacta y esté actualizada.	
	9.9.1.c Entreviste al personal para verificar que la lista de dispositivos se actualice cuando se agreguen, reubiquen, desactiven, etc., dispositivos.	
9.9.2 Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de	**9.9.2.a** Revise los procedimientos documentados para verificar que estén definidos para incluir lo siguiente: • Procedimientos para inspeccionar los dispositivos • Frecuencia de las inspecciones	Inspeccionar los dispositivos regularmente ayuda a las organizaciones a detectar con mayor rapidez la alteración o sustitución de un dispositivo y, por lo tanto, minimizar el posible impacto del uso de

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento). ***Nota:*** *Entre los ejemplos de indicios de que un dispositivo puede haber sido alterado o sustituido, se pueden mencionar accesorios inesperados o cables conectados al dispositivo, etiquetas de seguridad faltantes o cambiadas, carcasas rotas o con un color diferente o cambios en el número de serie u otras marcas externas.*	**9.9.2.b** Entreviste al personal responsable y observe los procesos de inspección para verificar lo siguiente: • El personal conoce los procedimientos para inspeccionar los dispositivos. • Todos los dispositivos se inspeccionan periódicamente para buscar indicios de alteraciones y sustitución.	dispositivos fraudulentos. El tipo de inspección dependerá del dispositivo, por ejemplo, se pueden usar fotografías de dispositivos conocidos por su seguridad y comparar la apariencia actual del dispositivo con la apariencia original para corroborar que no lo hayan cambiado. Otra opción puede ser usar un marcador seguro, como un marcador ultravioleta, para marcar la superficie y las ranuras del dispositivo para poder detectar, fácilmente, cualquier alteración o sustitución. Generalmente, los delincuentes reemplazan la carcasa externa del dispositivo para ocultar la alteración, y estos métodos ayudan a detectar estas actividades. Los proveedores de dispositivos también pueden brindar orientación sobre seguridad y “consejos prácticos” para determinar si el dispositivo ha sido alterado. La frecuencia de las inspecciones dependerá de factores, como la ubicación del dispositivo y si el dispositivo está o no bajo supervisión. Por ejemplo, los dispositivos que el personal de la organización deja en un área pública sin supervisión pueden tener más inspecciones que los que se encuentran en áreas seguras o que se supervisan cuando el público tiene acceso a ellos. El tipo y la frecuencia de las inspecciones las determina el comerciante, según lo estipulado en el proceso anual de evaluación de riesgos.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.9.3 Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos. La capacitación debe abarcar lo siguiente: • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).	**9.9.3.a** Revise el material de capacitación para el personal que trabaja en los puntos de venta para verificar que, en la capacitación, se incluya lo siguiente: • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad). **9.9.3.b** Entreviste a un grupo del personal del punto de venta para verificar que hayan recibido capacitación y que conozcan los procedimientos para realizar lo siguiente: • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).	Generalmente, los delincuentes fingirán ser personal de mantenimiento autorizado para poder acceder a los dispositivos de los POS (puntos de venta). Siempre se debe realizar una verificación de todas las personas externas que soliciten acceder a dispositivos antes de otorgarles la autorización, por ejemplo, corroborar con la gerencia o llamar por teléfono a la empresa de mantenimiento de POS (como el proveedor o adquiriente) para verificar. Muchos delincuentes intentarán engañar al personal y se vestirán para la ocasión (por ejemplo, pueden llevar una caja de herramientas y usar ropa de trabajo); también pueden tener información sobre la ubicación de los dispositivos; por eso, es importante que el personal esté capacitado para respetar los procedimientos en todo momento. Otro truco que usan los delincuentes es enviar un sistema de POS “nuevo” con instrucciones para cambiarlo por el sistema legítimo y “enviar” el sistema legítimo a la dirección especificada. Los delincuentes pueden llegar a proporcionar un franqueo pago, ya que están interesados en obtener estos dispositivos. El personal siempre debe verificar con el gerente o proveedor que el dispositivo sea legítimo y que provenga de una fuente confiable antes de instalarlo o usarlo en el negocio.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**9.10** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta y a los sistemas del CDE (entorno de datos del titular de la tarjeta).

Supervisar y evaluar las redes con regularidad

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta

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, la alerta y el análisis cuando algo no funciona bien. Determinar la causa de un riesgo es muy difícil, si no imposible, sin los registros de la actividad del sistema.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.1 Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.	**10.1** Verifique, mediante la observación y entrevistas al administrador del sistema, que se realice lo siguiente: • Las pistas de auditoría deben estar habilitadas y activas para los componentes del sistema. • El acceso a los componentes del sistema debe estar vinculado a usuarios específicos.	Es indispensable disponer de un proceso o sistema que vincule el acceso del usuario a los componentes del sistema a los que tuvieron acceso. El sistema genera registros de auditoría y proporciona la capacidad de rastrear actividades sospechosas hasta un usuario específico.
10.2 Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:	**10.2** Entreviste al personal responsable, observe los registros de auditoría, revise la configuración de los registros de auditoría y realice lo siguiente:	La generación de pistas de auditoría de actividades sospechosas alerta al administrador del sistema, envía datos a otros mecanismos de supervisión (como los sistemas de detección de intrusos) y proporciona una pista del historial para hacer seguimiento post-incidente. El registro de los siguientes eventos le permite a una organización identificar y rastrear actividades posiblemente malintencionadas.
10.2.1 Todo acceso por parte de usuarios a los datos del titular de la tarjeta.	**10.2.1** Verifique que se registre todo acceso de los usuarios a los datos del titular de la tarjeta.	Los individuos malintencionados podrían tener conocimiento sobre el uso de una cuenta de usuario con acceso a sistemas del CDE (entorno de datos del titular de la tarjeta) o podrían crear una cuenta nueva, no autorizada, para obtener acceso a los datos de los titulares de tarjetas. Un registro de todos los accesos individuales a los datos de los titulares de tarjetas puede identificar las cuentas que están en riesgo o que han sido mal utilizadas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos	**10.2.2** Verifique que se registren todas las acciones que realizan personas con privilegios administrativos o de raíz.	Las cuentas que tienen privilegios aumentados, como la cuenta “administrador” o “raíz”, tienen el potencial de afectar de manera relevante la seguridad o funcionalidad operacional de un sistema. Sin un registro de las actividades realizadas, la organización no puede rastrear los problemas que surjan por errores administrativos o por el uso fraudulento de privilegios hasta encontrar la acción y persona específicas.
10.2.3 Acceso a todas las pistas de auditoría	**10.2.3** Verifique que se registre el acceso a todas las pistas de auditoría.	Con frecuencia, las personas malintencionadas intentan modificar los registros de auditoría para ocultar sus acciones, por lo que llevar un registro de acceso le permite a una organización realizar un seguimiento de cualquier discrepancia o posible alteración de los registros de una cuenta individual. Tener acceso a los registros que identifican cambios, incorporaciones y eliminaciones puede ayudar a rastrear los pasos realizados por personal no autorizado.
10.2.4 Intentos de acceso lógico no válidos	**10.2.4** Verifique que se registren los intentos de acceso lógico no válidos.	Los individuos maliciosos frecuentemente realizarán múltiples intentos de acceso a los sistemas que sean su objetivo. Numerosos intentos de inicio de sesión no válidos pueden ser indicios de que un usuario no autorizado intenta utilizar “fuerza bruta” o adivinar una contraseña.
10.2.5 Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	**10.2.5.a** Verifique que se registre el uso de los mecanismos de identificación y autenticación.	Sin conocer quién tenía una sesión activa al momento de un incidente, es imposible identificar qué cuentas puedan haber sido utilizadas. Adicionalmente, los usuarios maliciosos pueden intentar manipular los controles de autenticación con el propósito de evitarlos o de suplantar la identidad de una cuenta válida.
	10.2.5.b Verifique que se registre todo aumento de privilegios.	
	10.2.5.c Verifique que se registren todos los cambios, incorporaciones y eliminaciones de cualquier cuenta con privilegios administrativos o de raíz.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.2.6 Inicialización, detención o pausa de los registros de auditoría	**10.2.6** Verifique que se registre lo siguiente: • Inicialización de los registros de auditoría. • Detención o pausa de los registros de auditoría.	Desactivar los registros de auditoría (o pausarlos) antes de que se realicen actividades ilícitas es una práctica común de los usuarios malintencionados que desean evitar ser detectados. La inicialización de registros de auditoría podría indicar que la función del registro fue inhabilitada por un usuario para ocultar sus acciones.
10.2.7 Creación y eliminación de objetos en el nivel del sistema	**10.2.7** Verifique que estén registradas la creación y la eliminación de objetos en el nivel del sistema.	El software malicioso, tal como el malware, a menudo crea o reemplaza objetos en el nivel de sistema en el sistema objetivo para controlar una función u operación particular en ese sistema. Si se registran los objetos en el nivel de sistema, como tablas de bases de datos o procedimientos almacenados, cuando se crean o se eliminan, será más fácil determinar si dichas modificaciones fueron autorizadas.
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 la observación de los registros de auditoría, realice lo siguiente para cada evento auditable (del punto 10.2):	Mediante el registro de estos detalles para los eventos auditables que contiene el punto 10.2, es posible identificar rápidamente un riesgo potencial y, con suficiente detalle conocer quién, qué, dónde, cuándo y cómo.
10.3.1 Identificación de usuarios	**10.3.1** Verifique que la identificación de usuario 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	**10.3.4** Verifique que la indicación de éxito o fallo se incluya en las entradas del registro.	
10.3.5 Origen del evento	**10.3.5** 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 recursos afectados.	**10.3.6** Verifique que la identidad o el nombre de los datos, de los componentes del sistema o de los recursos afectados se incluyan en las entradas del registro.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
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 NTP (protocolo de tiempo de red).*	**10.4** Revise las normas de configuración y los procesos para verificar que la tecnología de sincronización se implemente y mantenga actualizada, según los Requisitos 6.1 y 6.2 de las PCI DSS.	La tecnología de sincronización de tiempo se utiliza para sincronizar los relojes de múltiples sistemas. Cuando los relojes no están sincronizados correctamente, puede ser difícil, si no imposible, comparar archivos de registro de diferentes sistemas y establecer una secuencia de eventos exacta (indispensable para el análisis forense en el caso de una falla de seguridad). Para los equipos de investigaciones forenses posteriores al incidente, la exactitud y la uniformidad del tiempo en todos los sistemas y el tiempo de cada actividad resulta fundamental para determinar el grado en el que los sistemas estuvieron en riesgo.
10.4.1 Los sistemas críticos tienen un horario uniforme y correcto.	**10.4.1.a** Revise el proceso para adquirir, distribuir y guardar el horario correcto en la organización para verificar lo siguiente: • Solo los servidores horarios centrales designados reciben señales de hora de fuentes externas, y las señales de hora de fuentes externas se basan en el Tiempo Atómico Internacional o UTC. • Si hubiera más de un servidor de horario designado, estos se emparejan para mantener la hora exacta. • Los sistemas reciben información horaria solo de los servidores de horario central designados.	
	10.4.1.b Observe la configuración de los parámetros del sistema relacionados con la hora para obtener una muestra de los componentes del sistema y verificar lo siguiente: • Solo los servidores horarios centrales designados reciben señales de hora de fuentes externas, y las señales de hora de fuentes externas se basan en el Tiempo Atómico Internacional o UTC. • Si hubiera más de un servidor de horario designado, estos se emparejan para mantener la hora exacta. • Los sistemas reciben información horaria solo de los servidores horarios centrales designados.	
10.4.2 Los datos de tiempo están protegidos.	**10.4.2.a** Revise la configuración del sistema y los parámetros de configuración de sincronización para verificar que el acceso a los datos de la hora esté limitado solo al personal que tenga una necesidad comercial para acceder a los datos de la hora.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	10.4.2.b Revise la configuración del sistema, los registros y parámetros de configuración de sincronización y los procesos para verificar que todos los cambios en la configuración de la hora en los sistemas críticos se registren, supervisen y revisen.	
10.4.3 Los parámetros de la hora se reciben de fuentes aceptadas por la industria.	**10.4.3** Revise la configuración del sistema para verificar que los servidores de horario acepten actualizaciones de hora de fuentes externas específicas aceptadas por la industria (para evitar que personas malintencionadas cambien el reloj). De forma opcional, estas actualizaciones pueden cifrarse con una clave simétrica, y pueden crearse listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de hora (para evitar el uso no autorizado de servidores horarios internos).	
10.5 Proteja las pistas de auditoría para que no se puedan modificar.	**10.5** Entreviste a los administradores del sistema y revise los permisos y la configuración del sistema para verificar que las pistas de auditoría sean seguras y que no se puedan modificar de la siguiente manera:	A menudo, los individuos malintencionados que han ingresado a la red intentarán editar los registros de auditoría para ocultar su actividad. Sin la protección adecuada de los registros de auditoría, su integridad y exactitud no se pueden garantizar y los registros de auditoría se pueden considerar inútiles como herramienta de investigación después de una situación de riesgo.
10.5.1 Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.	**10.5.1** Solo aquellas personas que lo necesiten por motivos laborales pueden visualizar los archivos de las pistas de auditoría.	Una protección adecuada de los registros de auditoría incluye el control de acceso sólido (limitar el acceso a los registros solo a quienes “necesitan saber”) y el uso de segregación física o de red para que sea más difícil encontrar y modificar el registro. Realizar, rápidamente, una copia de seguridad de los registros en medios o servidores de registros centralizados que sean difíciles de alterar protege los registros, incluso si el sistema que genera los registros está en riesgo.
10.5.2 Proteja los archivos de las pistas de auditoría contra 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 mecanismos de control de acceso y la segregación física o de redes.	
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.	**10.5.3** Se realiza, oportunamente, una copia de seguridad de los archivos actuales de las pistas de auditoría en medios o servidores de registros centralizados que son difíciles de modificar.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.5.4 Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.	**10.5.4** Los registros para tecnologías externas (por ejemplo, tecnologías inalámbricas, *firewalls*, DNS, correo) se copian en medios o servidores de registros centralizados, internos y seguros.	Mediante la creación de registros de tecnologías externas, como tecnologías inalámbricas, *firewalls*, DNS y servidores de correo, el riesgo de que dichos registros se pierdan o modifiquen es menor, ya que están más seguros en la red interna. Los registros se pueden crear directamente en el medio o sistema interno seguro, o se pueden descargar o copiar desde sistemas externos.
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** Revise la configuración del sistema, los archivos monitoreados y los resultados de las actividades de supervisión para corroborar el uso del software de supervisión de integridad de archivos o de detección de cambios en los registros.	Los sistemas de supervisión de integridad de archivos o de detección de cambios verifican los cambios realizados en los archivos críticos y notifican se detectan cuando dichos cambios. Para efectos de supervisión de la integridad de archivos, una entidad generalmente supervisa los archivos que no cambian regularmente pero cuando cambian indican un riesgo potencial.
10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas. ***Nota:*** *Para cumplir con este requisito, se pueden usar herramientas de recolección, análisis y alerta de registros.*	**10.6** Realice lo siguiente:	Muchas violaciones a la seguridad ocurren varios días o meses antes de ser detectadas. Las revisiones regulares de registros realizadas con medios automáticos o por el personal sirven para identificar y abordar de manera proactiva el acceso no autorizado al entorno de datos del titular de la tarjeta. El proceso de revisión del registro no debe ser manual. Usar herramientas de recolección, análisis y alerta de registros facilita el proceso, ya que identifican cuáles son los eventos de registros que se deben revisar.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.6.1 Revise las siguientes opciones, al menos, una vez al día: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, *firewalls*, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).	**10.6.1.a** Revise las políticas y los procedimientos de seguridad para verificar que los procedimientos se definen para revisar lo siguiente, al menos, una vez al día, ya sea manualmente o con herramientas de registro: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, *firewalls*, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).	La verificación de los registros diariamente minimiza la cantidad de tiempo y exposición a una violación potencial de seguridad. Para identificar posibles problemas, es indispensable llevar a cabo una revisión diaria de los eventos de seguridad, por ejemplo, notificaciones o alertas que identifican actividades sospechosas o poco comunes, como de los registros de los componentes críticos del sistema, de los registros de sistemas que realizan funciones de seguridad, como *firewalls*, IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención), sistemas FIM (de supervisión de integridad de archivos), etc. Tenga en cuenta que la determinación de “evento de seguridad” varía de una organización a otra y puede incluir el tipo de tecnología, el lugar y la función del dispositivo. Es posible que las organizaciones deseen tener una referencia de tráfico “normal” para identificar conductas irregulares.
	10.6.1.b Observe los procesos y entreviste al personal para verificar que los siguientes puntos se controlen, al menos, una vez al día: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, *firewalls*, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).	
10.6.2 Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.	**10.6.2.a** Revise las políticas y los procedimientos de seguridad para verificar que estén definidos para realizar una revisión periódica de los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según la política y estrategia de gestión de riesgos de la organización.	Los registros de todos los demás componentes del sistema también se deben revisar periódicamente para identificar indicios de posibles problemas o intentos de acceder a sistemas confidenciales a través de sistemas menos confidenciales. La frecuencia de las revisiones se determina de acuerdo con la evaluación anual de riesgos de la entidad.
	10.6.2.b Revise la documentación de evaluación de riesgos de la organización y entreviste al personal para verificar que las revisiones se realicen en conformidad con las políticas y la estrategia de gestión de riesgos de la organización.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.6.3 Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.	**10.6.3.a** Revise las políticas y los procedimientos de seguridad para verificar que los procesos se definen para realizar un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.	Si no se investigan las excepciones y anomalías detectadas en el proceso de revisión de registros, es posible que la entidad no tenga conocimiento de las actividades no autorizadas y posiblemente malintencionadas presentes en su propia red.
	10.6.3.b Observe los procesos y entreviste al personal para verificar que se realice un seguimiento de las excepciones y anomalías.	
10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad).	**10.7.a** Revise las políticas y los procedimientos de seguridad y verifique que definan lo siguiente: • Políticas de retención de registros de auditoría • Procedimientos para conservar los registros de auditoría durante, al menos, un año, con un mínimo de disponibilidad en línea de tres meses.	La retención de registros por lo menos un año permite conservar información importante si se tiene en cuenta que a menudo toma cierto tiempo detectar que ha ocurrido una situación de riesgo y permite a los investigadores disponer de historial de registro suficiente para determinar mejor la duración de una violación potencial a la seguridad y los sistemas que hayan sido potencialmente afectados. Al tener tres meses de registros disponibles de manera inmediata, una entidad puede identificar y minimizar rápidamente el impacto de una violación de seguridad de los datos. Almacenar los registros en lugares externos evita que estén directamente disponibles; esto genera una demora al momento de recuperar datos de registros, realizar análisis e identificar sistemas o datos afectados.
	10.7.b Entreviste al personal y revise los registros de auditoría para verificar que estén disponible durante, al menos, un año.	
	10.7.c Entreviste al personal y observe los procesos para verificar que se puedan recuperar, al menos, los registros de los últimos tres meses para analizarlos.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.8 Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección y el informe oportunos de fallas de los sistemas de control de seguridad crítica, lo que incluye, sin carácter restrictivo, la falla de lo siguiente: • *Firewalls* • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan)	**10.8.a** Revise las políticas y los procedimientos documentados para verificar que estén definidos los procesos de detección oportuna y presentación de informes de las fallas de los sistemas críticos de control de seguridad, que incluyan entre otros fallas por: • *Firewalls* • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan)	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Sin procesos formales para detectar y alertar cuando fallan los controles de seguridad crítica, las fallas pueden pasar desapercibidas durante períodos prolongados y proporcionar a los atacantes tiempo suficiente para poner en riesgo los sistemas y robar datos confidenciales del entorno de datos de titulares de tarjetas. Los tipos específicos de fallas pueden variar dependiendo de la función del dispositivo y la tecnología en uso. Las fallas típicas incluyen a un sistema que deja de realizar su función de seguridad o que no funciona como debe ser; por ejemplo, un *firewall* que borra todas sus reglas o que sale fuera de línea.
	10.8.b Revise los procesos de detección y de alerta y entreviste al personal para verificar que los procesos se implementan para todos los controles de seguridad críticos, y que la falla de un control de seguridad críticos da lugar a la generación de una alerta.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.8.1 ***Requisitos adicionales solo para los proveedores de servicios*****:** Responder a las fallas de los controles de seguridad críticos en el momento oportuno. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: • Restaurar las funciones de seguridad • Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad • Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz • Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad • Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad • Implementar controles para prevenir que se vuelva a producir la causa de la falla • Reanudar la supervisión de los controles de seguridad	**10.8.1.a** Revise las políticas y procedimientos documentados y entreviste al personal para verificar que los procesos están definidos e implementados para responder a una falla del control de seguridad, e incluya: • Restaurar las funciones de seguridad • Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad • Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz • Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad • Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad • Implementar controles para prevenir que se vuelva a producir la causa de la falla • Reanudar la supervisión de los controles de seguridad **10.8.1.b** Revise los registros para verificar que se documentan las fallas del control de seguridad para incluir: • Identificación de las causas de la falla, incluida la causa raíz • Duración (fecha y hora de inicio y fin) de la falla de seguridad • Detalles de la remediación necesaria para abordar la causa raíz	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Si no se responde a las alertas de las fallas críticas del control de seguridad de manera rápida y efectiva, los atacantes pueden utilizar este tiempo para insertar software malicioso, tomar control de un sistema, o robar datos del entorno de la entidad. La evidencia documentada (por ejemplo, registros dentro de un sistema de gestión de problemas) deberá apoyar que los procesos y procedimientos están implementados para responder a las fallas de seguridad. Además, el personal debe estar al tanto de sus responsabilidades en el caso de una falla. Las medidas y las respuestas a la falla deben capturarse en la evidencia documentada.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
10.9 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**10.9** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos diarios para monitorear todo acceso a los recursos de la red y a los datos del titular de la tarjeta.

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

Las vulnerabilidades son descubiertas continuamente por personas malintencionadas e investigadores y son introducidas mediante software nuevo. Los componentes del sistema, los procesos y el software personalizado deben evaluarse con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados. ***Nota:*** *Los métodos que pueden utilizarse en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC o IDS/IPS inalámbricos.* *Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.*	**11.1.a** Revise las políticas y los procedimientos para verificar que los procesos estén definidos para detectar e identificar, trimestralmente, puntos de acceso inalámbricos autorizados y no autorizados. **11.1.b** Verifique que la metodología sea la adecuada para detectar e identificar cualquier punto de acceso inalámbrico no autorizado, que incluya, al menos, lo siguiente: • Tarjetas WLAN insertadas en los componentes del sistema • Dispositivos portátiles o móviles conectados a los componentes del sistema para crear puntos de acceso inalámbricos (por ejemplo, mediante USB, etc.). • Dispositivos inalámbricos conectados a un puerto o a un dispositivo de red. **11.1.c** Si se realiza un análisis inalámbrico, revise el resultado de los últimos análisis inalámbricos para verificar lo siguiente: • Se identifican los puntos de acceso inalámbricos autorizados y no autorizados. • El análisis se realiza, al menos, trimestralmente en todos los componentes del sistema y en todas las instalaciones. **11.1.d** Si se utiliza la supervisión automatizada (por ejemplo, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención] inalámbricos, NAC [control de acceso a la red], etc.), verifique que la configuración genere alertas para notificar al personal.	La implementación o el uso indebido de tecnología inalámbrica dentro de una red es uno de los medios más comunes que usan las personas malintencionadas para acceder a la red y a los datos del titular de la tarjeta. Si un dispositivo inalámbrico o una red inalámbrica se instala sin el conocimiento de la empresa, un atacante podría ingresar fácilmente y sin ser vista a la red. Los dispositivos inalámbricos no autorizados pueden estar ocultos en una computadora o en otro componente del sistema, o conectados a estos; o bien pueden estar conectados directamente a un puerto o dispositivo de red, como un conmutador o router. Cualquier dispositivo no autorizado podría generar un punto de acceso no autorizado en el entorno. Conocer cuáles son los dispositivos inalámbricos autorizados ayuda a los administradores a identificar, rápidamente, los dispositivos no autorizados; y actuar ante la identificación de puntos de acceso inalámbricos no autorizados ayuda a minimizar de manera proactiva la exposición del CDE (entorno de datos del titular de la tarjeta) a personas malintencionadas. Debido a la facilidad con la que un punto de acceso inalámbrico puede conectarse a una red, la dificultad para detectar su presencia y el gran riesgo que presentan los dispositivos inalámbricos no autorizados, estos análisis deben realizarse incluso cuando existe una política que prohíbe el uso de tecnología inalámbrica. El tamaño y la complejidad de un entorno

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
		particular determinarán las herramientas y los procesos apropiados que han de utilizarse para proporcionar garantía suficiente de que no se ha instalado un punto de acceso inalámbrico no autorizado en el entorno.
11.1.1 Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada.	**11.1.1** Revise los registros documentados para verificar que se conserve un inventario de los puntos de acceso inalámbricos autorizados y que se documente una justificación comercial para todos los puntos de acceso inalámbricos autorizados.	***Por ejemplo:*** *En caso de un quiosco minorista independiente en un centro comercial, donde todos los componentes de comunicación se encuentran en carcasas a prueba de manipulaciones o en las que estas serían muy notorias, realizar una inspección física detallada del quiosco puede bastar para asegurarse de que no se haya conectado o instalado un punto de acceso inalámbrico no autorizado. Sin embargo, en un entorno con numerosos nodos (como en el caso de grandes tiendas minoristas, centros de llamadas, salas de servidores o centros de datos), es más difícil realizar una inspección física minuciosa. En este caso, se pueden combinar múltiples métodos para cumplir con el requisito, como realizar inspecciones físicas del sistema en conjunto con los resultados de un analizador inalámbrico.*
11.1.2 Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados.	**11.1.2.a** Revise el plan de respuesta a incidentes de la organización (Requisito 12.10) para verificar que defina y solicite una respuesta en caso de detectar puntos de acceso inalámbricos no autorizados.	
	11.1.2.b Entreviste al personal responsable e inspeccione los análisis inalámbricos recientes y las respuestas correspondientes para verificar que se tomen medidas cuando se encuentren puntos de acceso inalámbricos no autorizados.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.2 Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de *firewall*, actualizaciones de productos). ***Nota:*** *Pueden combinarse varios informes de análisis para el proceso de análisis trimestral, a fin de demostrar que se analizaron todos los sistemas y que se abordaron todas las vulnerabilidades aplicables. Podría solicitarse documentación adicional para verificar que las vulnerabilidades no resueltas estén en proceso de resolverse.* *Para el cumplimiento inicial de las PCI DSS, no es necesario tener cuatro análisis trimestrales aprobados si el asesor verifica que 1) el resultado del último análisis fue aprobado, 2) la entidad ha documentado las políticas y los procedimientos que disponen la realización de análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En los años posteriores a la revisión inicial de la PCI DSS, debe haber cuatro análisis trimestrales aprobados.*	**11.2** Revise los informes de análisis y la documentación de respaldo para verificar que se realicen análisis de las vulnerabilidades internas y externas de la siguiente manera:	Un análisis de vulnerabilidades es una combinación de herramientas, técnicas y/o métodos manuales o automáticos que se ejecuta en servidores y dispositivos de red internos y externos, y está diseñado para exponer posibles vulnerabilidades que pueden encontrar y aprovechar personas malintencionadas. Existen tres tipos de análisis de vulnerabilidades que disponen las PCI DSS: • Análisis trimestral de vulnerabilidades internas realizado por personal calificado (no es necesario usar un ASV [proveedor aprobado de escaneo] certificado por el PCI SSC). • Análisis trimestral de vulnerabilidades externas realizado por un ASV (proveedor aprobado de escaneo). • Análisis externo e interno, según sea necesario, después de cambios significativos. Después de identificar estas debilidades, la entidad las corrige y repite el análisis hasta corregir todas las vulnerabilidades. La identificación y el tratamiento de vulnerabilidades oportunamente reducen la probabilidad de explotación de una vulnerabilidad y la posible exposición a riesgo de un componente del sistema o de datos de titulares de tarjetas.
11.2.1 Realice análisis interno de vulnerabilidades trimestralmente. Aborde las vulnerabilidades y realice	**11.2.1.a** Revise los informes de análisis y verifique que se hayan realizado cuatro análisis trimestrales internos en los últimos 12 meses.	Un proceso establecido para identificar vulnerabilidades en sistemas internos requiere que los análisis de vulnerabilidades se realicen

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
redigitalizaciones para verificar que todas las vulnerabilidades de “alto riesgo” se resuelven de acuerdo con la clasificación de la vulnerabilidad de la entidad (según el Requisito 6.1). Los análisis deben estar a cargo de personal calificado.	**11.2.1.b** Revise los informes de los análisis y verifique que el proceso incluya la repetición de los análisis hasta que se corrijan todas las vulnerabilidades “de alto riesgo”, según las disposiciones del Requisito 6.1 de las PCI DSS.	trimestralmente. Las vulnerabilidades que suponen el mayor riesgo para el entorno (por ejemplo, las clasificadas como “altas” según el Requisito 6.1) son las que tienen más prioridad para corregirse.
	11.2.1.c Entreviste al personal para verificar que el análisis lo haya realizado un recurso interno calificado o personal externo capacitado y, si corresponde, que la persona que realice la prueba tenga independencia organizativa (no es necesario que sea un QSA o ASV).	Los análisis de vulnerabilidades internas pueden estar a cargo de personal interno calificado que sea razonablemente independiente de los componentes del sistema analizados (por ejemplo, un administrador de *firewall* no puede analizar el *firewall*), o una entidad puede elegir que una empresa especializada en análisis realice los análisis de vulnerabilidades internas.
11.2.2 Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI *Security Standards Council*). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados. ***Nota:*** *Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor aprobado de análisis (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC).* *Consulte la Guía del programa de ASV (proveedor aprobado de escaneo) publicada en el sitio web del PCI SSC para obtener información sobre las responsabilidades de análisis del cliente, sobre la preparación del análisis, etc.*	**11.2.2.a** Revise los resultados de los últimos cuatro análisis trimestrales de vulnerabilidades externas y verifique que se hayan realizado cuatro análisis trimestrales de vulnerabilidades externas en los últimos 12 meses.	Debido a que las redes externas son la mayor probabilidad de riesgo, el análisis externo de vulnerabilidades trimestral debe ser realizado por un Proveedor aprobado de análisis (ASV) de las PCI SSC. Un programa de detección robusta garantiza que las detecciones se realizan y que las vulnerabilidades se abordan de manera oportuna.
	11.2.2.b Revise los resultados de cada análisis trimestral y repita los análisis para verificar que se hayan cumplido los requisitos de la Guía del programa de ASV (proveedor aprobado de escaneo) para obtener un análisis aprobado (por ejemplo, que no haya vulnerabilidades con una puntuación CVSS de 4.0 o superior y que no haya fallas automáticas).	
	11.2.2.c Revise los informes de análisis para verificar que los haya realizado un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.2.3 Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado.	**11.2.3.a** Inspeccione y coteje la documentación del control de cambios y los informes de análisis para verificar que se hayan analizado los componentes del sistema que hayan tenido cambios significativos.	La determinación de qué constituye un cambio significativo depende totalmente de la configuración de cada entorno. Si una actualización o modificación llegara a permitir el acceso a los datos del titular de la tarjeta o afectar la seguridad del entorno de datos del titular de la tarjeta, se la puede considerar un cambio significativo. Analizar un entorno después de realizar cambios significativos asegura que esos cambios se realizaron apropiadamente de tal manera que la seguridad del entorno no se haya puesto en riesgo como resultado del cambio. Se deben analizar todos los componentes del sistema afectados por el cambio.
	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: • No se hayan registrado vulnerabilidades con puntuaciones CSVV de 4.0 o superior en análisis externos. • Se hayan corregido todas las vulnerabilidades “de alto riesgo”, según lo estipulado en el Requisito 6.1 de las PCI DSS, en los análisis internos.	
	11.2.3.c Verifique que el análisis lo haya realizado un recurso interno calificado o personal externo capacitado y, si corresponde, que la persona que realiza la prueba tenga independencia organizativa (no es necesario que sea un QSA o ASV).	
11.3 Implemente una metodología para las pruebas de penetración que incluya lo siguiente: • Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). • Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. • Incluya pruebas del entorno interno y externo de la red. • Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. • Defina las pruebas de penetración de	**11.3** Revise la metodología de pruebas de penetración y entreviste al personal responsable para verificar que se implemente la metodología e incluya lo siguiente: • Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). • Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. • Incluya pruebas del entorno interno y externo de la red. • Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. • Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. • Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las	El objetivo de una prueba de penetración es simular una situación de ataque real con el fin de identificar qué tan lejos podría llegar el atacante al penetrar un entorno. Esto le permite a la entidad comprender mejor su posible exposición y desarrollar una estrategia para protegerse contra los ataques. Una prueba de penetración difiere de un análisis de vulnerabilidades; ya que es un proceso activo que puede incluir aprovechar las vulnerabilidades identificadas. Uno de los primeros pasos que tomará quien realiza la prueba de penetración es llevar a cabo un análisis de vulnerabilidades a fin de organizar una estrategia de pruebas, aunque no será el único paso. Incluso si un análisis de vulnerabilidades no detecta vulnerabilidades conocidas, con frecuencia, el encargado de la

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. • Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. • Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. • Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.	funciones de red y los sistemas operativos. • Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. • Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.	prueba de penetración adquiere los conocimientos necesarios sobre el sistema para identificar posibles deficiencias en la seguridad. La prueba de penetración suele ser un proceso sumamente manual. Si bien se pueden utilizar algunas herramientas automatizadas, el encargado de la prueba utilizará sus conocimientos sobre sistemas para penetrar en un entorno. Comúnmente, el encargado de la prueba encadena varios tipos de ataques con el objetivo de penetrar a través de capas de defensas. Por ejemplo, si el encargado de la prueba encuentra un medio para obtener acceso a un servidor de aplicaciones, entonces usarán el servidor en riesgo como punto para escenificar un nuevo ataque basándose en los recursos a los que el servidor tiene acceso. De esta manera, el encargado de la prueba puede simular los métodos implementados por un atacante con el fin de identificar áreas posiblemente débiles en el entorno. *Las técnicas de las pruebas de penetración son diferentes en cada organización, y el tipo, la profundidad y la complejidad de las pruebas dependerán del entorno específico y de la evaluación de riesgos de la organización.*
11.3.1 Lleve a cabo pruebas de penetración *externas*, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).	**11.3.1.a** Revise el alcance del trabajo y los resultados de la última prueba de penetración externa para verificar que se realice de la siguiente manera: • Según la metodología definida. • Por lo menos, anualmente • Después de cualquier cambio significativo en el entorno.	Llevar a cabo pruebas de penetración regularmente y después de implementar cambios significativos en el entorno es una medida de seguridad preventiva que ayuda a minimizar el posible acceso al CDE (entorno de datos del titular de la tarjeta) por parte de personas malintencionadas. La determinación de qué constituye una actualización o modificación significativa depende totalmente de la configuración de cada entorno. Si una actualización o modificación llegara a permitir el acceso a los datos del titular de la tarjeta o
	11.3.1.b Verifique que la prueba la haya realizado un recurso interno calificado o un empleado externo capacitado y, si corresponde, que la persona que realiza la prueba tenga independencia organizativa (no es necesario que sea	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	un QSA o ASV).	afectar la seguridad del entorno de datos del titular de la tarjeta, se la puede considerar un cambio significativo. Llevar a cabo pruebas de penetración después de una actualización o modificación en la red garantiza que los controles existentes seguirán funcionando correctamente después de implementar la actualización o modificación.
11.3.2 Lleve a cabo pruebas de penetración *internas*, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).	**11.3.2.a** Revise el alcance del trabajo y los resultados de la última prueba de penetración interna para verificar que se realice de la siguiente manera: • Según la metodología definida. • Por lo menos, anualmente • Después de cualquier cambio significativo en el entorno.	
	11.3.2.b Verifique que la prueba la haya realizado un recurso interno calificado o un empleado externo capacitado y, si corresponde, que la persona que realiza la prueba tenga independencia organizativa (no es necesario que sea un QSA o ASV).	
11.3.3 Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones.	**11.3.3** Revise los resultados de las pruebas de penetración para verificar que se hayan corregido las vulnerabilidades de seguridad detectadas y que la repetición de las pruebas confirme que las vulnerabilidades se corrigieron.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.3.4 Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, realice pruebas de penetración, al menos, una vez al año y después de implementar cambios en los métodos o controles de segmentación para verificar que los métodos de segmentación sean operativos y efectivos, y que aíslen todos los sistemas fuera de alcance de los sistemas en el CDE.	**11.3.4.a** Revise los controles de segmentación y revise la metodología de las pruebas de penetración para verificar que los procedimientos estén definidos para comprobar todos los métodos de segmentación y confirmar que son operativos y eficaces, y que, además, aíslan todos los sistemas fuera de alcance de los sistemas en el CDE. **11.3.4.b** Examinar los resultados de la prueba de penetración más reciente para verificar que: • La prueba de penetración para verificar los controles de segmentación se realiza al menos una vez al año y tras cualquier cambio en los controles o métodos de segmentación. • La prueba de penetración abarca todos los controles o métodos de segmentación implementados. • La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE. **11.3.4.c** Verifique que la prueba la haya realizado un recurso interno capacitado o un empleado externo cualificado y, si corresponde, que la persona que realiza la prueba tenga independencia organizativa (no es necesario que sea un QSA o ASV).	Las pruebas de penetración son una herramienta importante que sirve para confirmar la eficacia de las segmentaciones implementadas para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes. Las pruebas de penetración se deben centrar en los controles de segmentación, tanto de la red externa de la entidad como de la interna, pero fuera del CDE (entorno de datos del titular de la tarjeta), a fin de corroborar que no se pueden burlar los controles de segmentación para acceder al CDE (entorno de datos del titular de la tarjeta). Por ejemplo, realizar un análisis o prueba de red en busca de puertos abiertos para verificar que no hay conectividad entre las redes dentro del alcance y fuera del alcance.
11.3.4.1 ***Requisitos adicionales solo para los proveedores de servicios*:** Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación al menos cada seis meses, y después de cualquier cambio a los controles/métodos de segmentación.	**11.3.4.1.a** Revise los resultados de la prueba de penetración más reciente para verificar que: • La prueba de penetración para verificar los controles de segmentación se realiza al menos cada seis meses y tras cualquier cambio en los controles/métodos de segmentación. • La prueba de penetración abarca todos los controles o métodos de segmentación implementados. • La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE.	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Para los proveedores de servicios, la validación del alcance de la PCI DSS deberá llevarse a cabo con tanta frecuencia como sea posible para garantizar que el alcance de la PCI DSS se mantenga actualizado y alineado con los objetivos comerciales cambiantes.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
	11.3.4.1.b Verifique que la prueba la haya realizado un recurso interno capacitado o un empleado externo cualificado y, si corresponde, que la persona que realiza la prueba tenga independencia organizativa (no es necesario que sea un QSA o ASV).	
11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Supervisar todo el tráfico presente en el perímetro y en los puntos críticos del entorno de datos de titulares de tarjetas y alertar al personal ante la sospecha de riesgos. Mantener actualizados todos los motores, bases y firmas de detección y prevención de intrusiones.	**11.4.a** Revise la configuración del sistema y los diagramas de red para verificar que se implementen técnicas (como los sistemas de intrusión-detección y de intrusión-prevención) para monitorear todo el tráfico en los siguientes lugares: • En el perímetro del entorno de datos del titular de la tarjeta. • En los puntos críticos del entorno de datos del titular de la tarjeta.	Las técnicas de intrusión-detección y de intrusión-prevención (como las IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención]) comparan el tráfico que proviene de la red con “firmas” conocidas o conductas de miles de tipos de exposiciones (herramientas de hackers, troyanos y otros software maliciosos) y envían alertas o detienen el intento cuando ocurre. Sin un enfoque proactivo que detecte las actividades no autorizadas, los ataques a recursos informáticos (o el uso indebido) pueden pasar inadvertidos en tiempo real. Las alertas de seguridad que generan estas técnicas se deben monitorear para poder detener los intentos de intrusiones.
	11.4.b Revise la configuración del sistema y entreviste al personal responsable para confirmar que las técnicas de intrusión-detección y de intrusión-prevención alerten al personal de posibles riesgos.	
	11.4.c Revise la configuración de las IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) y la documentación del proveedor para verificar que las técnicas de intrusión-detección y de intrusión-prevención se configuren, conserven y actualicen según las instrucciones del proveedor para garantizar una protección óptima.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de integridad de archivos) para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana. *(continúa en la página siguiente)*	**11.5.a** Verifique que se implemente el uso de un mecanismo de detección de cambios mediante la observación de la configuración del sistema y los archivos monitoreados, así como la revisión de los resultados de las actividades de supervisión. Ejemplos de archivos que deben supervisarse: • Ejecutables del sistema • Ejecutables de aplicaciones • Archivos de configuración y parámetros • Archivos de almacenamiento central, históricos o archivados, de registro y auditoría • Archivos críticos adicionales que determine la entidad (por ejemplo, a través de la evaluación de riesgos u otros medios)	Las soluciones de detección de cambios, como la FIM (supervisión de integridad de archivos), verifican los cambios, adiciones y eliminaciones en los archivos críticos y notifican cuando detectan dichos cambios. Si la solución de detección de cambios no se implementa correctamente y no se controlan sus resultados, una persona malintencionada podría alterar, añadir o eliminar el contenido de los archivos de configuración, los programas del sistema operativo o los ejecutables de la aplicación. Si no se detectan los cambios no autorizados, es posible que los controles de seguridad existentes se tornen ineficientes o que se produzca el robo de los datos del titular de la tarjeta sin un impacto perceptible en el procesamiento normal.
Nota: *A los fines de la detección de cambios, los archivos críticos suelen ser aquellos que no se modifican con regularidad, pero cuya modificación podría implicar un riesgo o peligro para el sistema. Los mecanismos de detección de cambios, como los productos de supervisión de integridad de archivos, suelen estar 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.b** Verifique que el mecanismo esté configurado para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos, y para realizar comparaciones de archivos críticos, al menos, semanalmente.	
11.5.1 Implemente un proceso para responder a las alertas que genera la solución de detección de cambios.	**11.5.1** Entreviste al personal para verificar que todas las alertas se investiguen y resuelvan.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
11.6 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	**11.6** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.	El personal debe conocer y respetar siempre las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad.

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 al personal lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de sus responsabilidades para protegerlos. A los fines del Requisito 12, el término “personal” hace referencia a los empleados de tiempo completo y parcial, a los empleados temporales, a los contratistas y consultores que “residen” en las instalaciones de la entidad o que tienen acceso al entorno de datos del titular de la tarjeta.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.1 Establezca, publique, mantenga y distribuya una política de seguridad.	**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).	La política de seguridad de la información de una empresa crea un plan de acción para implementar medidas de seguridad para proteger su activo más valioso. Todo el personal debe estar al tanto de la confidencialidad de los datos y de sus responsabilidades para protegerlos.
12.1.1 Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno.	**12.1.1** Verifique que la política de seguridad de la información se revise, al menos, una vez al año y se actualice cuando sea necesario, de manera que refleje los cambios en los objetivos del negocio o en el entorno de riesgos.	Las amenazas a la seguridad y los métodos de protección evolucionan rápidamente. Si la política de seguridad no se actualiza para reflejar estos cambios importantes, no se implementarán nuevas medidas de protección para luchar contra estas amenazas.
12.2 Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: • Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.). • Identifica activos críticos, amenazas y vulnerabilidades. • Los resultados en un análisis formal y documentado de riesgo. *Los ejemplos de metodologías de evaluación de riesgos incluyen, entre otros, OCTAVE, ISO 27005 y NIST SP 800-30.*	**12.2.a** Verifique que se documenta un proceso anual de evaluación de riesgos que: • Identifica activos críticos, amenazas y vulnerabilidades. • Resultados en un análisis formal y documentado de riesgo **12.2.b** Revise la documentación de la evaluación de riesgos para verificar que el proceso de evaluación de riesgos se ejecute, al menos, una vez al año y después de cambios significativos en el entorno.	Una evaluación de riesgos le permite a la organización identificar las amenazas y las vulnerabilidades asociadas que pueden tener un impacto negativo en el negocio. Ejemplos de diferentes consideraciones de riesgo incluyen a los delitos informáticos, los ataques web, y el malware de POS. Los recursos pueden asignarse de forma efectiva a fin de implementar controles que reduzcan la probabilidad o la posible incidencia de la amenaza detectada. Llevar a cabo evaluaciones de riesgos, al menos, anualmente y después de cambios significativos le permite a la organización estar actualizada en lo que respecta a cambios organizativos y a las cambiantes amenazas, tendencias y tecnologías.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.3 Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente. ***Nota:*** *Ejemplos de tecnologías críticas incluyen, entre otros, las tecnologías inalámbricas y de acceso remoto, las computadoras portátiles, las tabletas, los medios electrónicos extraíbles, el uso del correo electrónico y el uso de Internet.* Asegúrese de que estas políticas de uso requieran lo siguiente:	**12.3** Revise las políticas de uso de las tecnologías críticas y entreviste al personal responsable para verificar que se implementen las siguientes políticas y de la siguiente manera:	Las políticas de uso por parte del personal pueden prohibir el uso de ciertos dispositivos y otras tecnologías si es la política de la empresa, o proporcionar una guía para el personal a propósito de la utilización e implementación correctas. Si las políticas de uso no están implementadas, el personal puede utilizar las tecnologías para transgredir la política de la empresa, lo que permitiría que personas malintencionadas obtengan acceso a sistemas y datos de titulares de sistemas críticos.
12.3.1 Aprobación explícita de las partes autorizadas	**12.3.1** Verifique que las políticas de uso incluyan procesos para la aprobación explícita de partes autorizadas para utilizar las tecnologías.	Sin una solicitud de aprobación apropiada para la implementación de estas tecnologías, un miembro del personal puede inocentemente implementar una solución a una necesidad de negocio percibida, pero al mismo tiempo abrir un enorme agujero que exponga los sistemas y datos críticos a personas malintencionadas.
12.3.2 Autenticación para el uso de la tecnología	**12.3.2** Verifique que las políticas de uso incluyan procesos que autentiquen el uso de todas las tecnologías con ID de usuario y contraseña u otro elemento de autenticación (por ejemplo, *token*).	Si se implementan tecnologías sin la debida autenticación (ID de usuarios y contraseñas, *tokens*, VPN, etc.), personas malintencionadas pueden fácilmente utilizar estas tecnologías desprotegidas para acceder a sistemas críticos y datos de titulares de tarjetas.
12.3.3 Lista de todos los dispositivos y el personal que tenga acceso	**12.3.3** Verifique que las políticas de uso definen: • Una lista de todos los dispositivos críticos, y • Una lista del personal autorizado para utilizar los dispositivos.	Las personas malintencionadas pueden violar la seguridad física y colocar sus propios dispositivos en la red como una “puerta trasera”. El personal también puede evadir procedimientos e instalar dispositivos. Un inventario fiable con el debido etiquetado de dispositivos permite identificar rápidamente las instalaciones no aprobadas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.3.4 Método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos).	**12.3.4** Verifique que las políticas de uso definan un método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetados, codificación o inventario de dispositivos).	Las personas malintencionadas pueden violar la seguridad física y colocar sus propios dispositivos en la red como una “puerta trasera”. El personal también puede evadir procedimientos e instalar dispositivos. Un inventario fiable con el debido etiquetado de dispositivos permite identificar rápidamente las instalaciones no aprobadas. Evalúe la posibilidad de establecer una convención oficial para designar los dispositivos, y registre todos los dispositivos de acuerdo con los controles de inventario establecidos. Se debe emplear un etiquetado lógico que contenga información, como códigos que correlacionen el dispositivo con su propietario, información de contrato y objetivo.
12.3.5 Usos aceptables de la tecnología	**12.3.5** Verifique que las políticas de uso definan los usos aceptables de la tecnología.	Al definir el uso dentro del negocio y la ubicación aceptables de los dispositivos y la tecnología aprobados por la empresa, ésta se encuentra en mejor posición para administrar y controlar brechas de configuraciones y controles operativos, a fin de asegurar que no se abra una “puerta trasera” para que una persona malintencionada obtenga acceso a sistemas críticos y datos de titulares de tarjetas.
12.3.6 Ubicaciones aceptables de las tecnologías en la red	**12.3.6** Verifique que las políticas de uso definan las 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 incluyan una lista de los 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 en las tecnologías de acceso remoto después de un período específico de inactividad.	Las tecnologías de acceso remoto son "puertas traseras" frecuentes para recursos críticos y datos de titulares de tarjetas. Al desconectar las tecnologías de acceso remoto cuando no se utilizan (por ejemplo, las que usa su proveedor de punto de venta, otros proveedores o socios comerciales para respaldar sus sistemas), se minimizan los riesgos y el acceso a las redes.
	12.3.8.b Revise la configuración de las tecnologías de acceso remoto para verificar que las sesiones de acceso remoto se desconecten automáticamente después de un período específico de inactividad.	
12.3.9 Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso	**12.3.9** Verifique que las políticas de uso requieran la activación de las tecnologías de acceso remoto que usan los proveedores y socios comerciales solo cuando se necesiten y que se desactiven automáticamente después de usarlas.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.3.10 En el caso del personal que tiene acceso a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad comercial definida. Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección de los datos de conformidad con los requisitos correspondientes de las PCI DSS.	**12.3.10.a** Verifique que las políticas de uso prohíban copiar, mover o almacenar datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto. **12.3.10.b** En el caso del personal que cuenta con la autorización correcta, verifique que las políticas de uso dispongan que los datos del titular de la tarjeta se protejan de conformidad con los requisitos de las PCI DSS.	Para asegurarse de que todo el personal sepa que no debe almacenar ni copiar datos del titular de la tarjeta en sus computadoras personales locales ni otros medios, la política debe prohibir, claramente, dichas actividades, a excepción del personal autorizado explícitamente para hacerlo. El almacenamiento o las copias de los datos del titular de la tarjeta en unidades de disco local o en otros medios se debe realizar de conformidad con los requisitos correspondientes 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.a** Verifique que las políticas de seguridad de la información definan, con claridad, las responsabilidades de seguridad de la información de todo el personal. **12.4.b** Entreviste a un grupo de empleados responsables y verifique que comprendan las políticas de seguridad.	Sin la asignación de roles de seguridad ni responsabilidades claramente definidas, podría haber una interacción que no concuerde con el grupo de seguridad, lo que podría tener como resultado la implementación no segura de tecnologías o el uso desactualizado o no seguro de tecnologías.
12.4.1 ***Requisitos adicionales solo para los proveedores de servicios:*** La gerencia ejecutiva deberá establecer la responsabilidad de la protección de los datos del titular de la tarjeta y un programa	**12.4.1.a** Revise la documentación para verificar que la gerencia ejecutiva ha asignado la responsabilidad general de mantener el cumplimiento de la PCI DSS de la entidad.	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* La asignación de la gerencia ejecutiva de las responsabilidades de cumplimiento de la PCI DSS

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
de cumplimiento de la PCI DSS para incluir: • Responsabilidad general de mantener el cumplimiento de la PCI DSS • Definir un estatuto para el programa de cumplimiento de la PCI DSS y la comunicación a la gerencia ejecutiva	**12.4.1.b** Revise el estatuto de la PCI DSS de la empresa para verificar que se describen las condiciones en las que se organiza y se comunica a la gerencia ejecutiva el programa de cumplimiento de la PCI DSS.	garantiza la visibilidad a nivel ejecutivo en el programa de cumplimiento de la PCI DSS y permite la oportunidad de hacer preguntas adecuadas para determinar la eficacia del programa e influir en las prioridades estratégicas. La responsabilidad general del programa de cumplimiento de la PCI DSS puede ser asignada a los roles individuales y/o a las unidades de negocio dentro de la organización. La gerencia ejecutiva puede incluir puestos de nivel C, junta directiva, o equivalente. Los títulos específicos dependerán de la estructura de la organización en particular. El nivel de detalle proporcionado a la gerencia ejecutiva deberá ser apropiado para la organización y el público objetivo en particular.
12.5 Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información:	**12.5** Revise los procedimientos y las políticas de seguridad de la información para verificar lo siguiente: • La asignación formal de la seguridad de la información a un Jefe de seguridad u a otro miembro de la gerencia relacionado con la seguridad. • Las siguientes responsabilidades de seguridad de la información se asignan de manera formal y específica:	Cada persona o equipo con responsabilidades sobre la administración de seguridad de la información debe ser claramente consciente de sus responsabilidades y tareas relacionadas a través de una política específica. Sin esta responsabilidad, las brechas de los procesos pueden abrir accesos a recursos críticos y a los datos del titular de la tarjeta. Las entidades también deberán tener en cuenta los planes de transición y/o sucesión para el personal clave para evitar posibles brechas en las tareas de seguridad, lo que podría dar lugar a responsabilidades que no están asignadas y por lo tanto no realizadas.
12.5.1 Establezca, documente y distribuya las políticas y los procedimientos de seguridad.	**12.5.1** Verifique que la responsabilidad de establecer, documentar y distribuir las políticas y los procedimientos de seguridad se asigne formalmente.	
12.5.2 Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente.	**12.5.2** Verifique que la responsabilidad de monitorear y analizar las alertas de seguridad y de distribuir la información al personal de las unidades comerciales y de seguridad se haya asignado formalmente.	
12.5.3 Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones.	**12.5.3** Verifique que la responsabilidad de establecer, documentar y distribuir los procedimientos de escalamiento y de respuesta ante incidentes de seguridad se asigne formalmente.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.5.4 Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.	**12.5.4** Verifique que la responsabilidad de administrar (agregar, eliminar y modificar) las cuentas de usuario y la administración de la autenticación esté asignada formalmente.	
12.5.5 Monitoree y controle todo acceso a los datos.	**12.5.5** Verifique que la responsabilidad de monitorear y controlar todo acceso a los datos esté formalmente asignada.	
12.6 Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta.	**12.6.a** Revise el programa de concienciación sobre seguridad para verificar que ayuda a que todo el personal tome conciencia sobre la política y los procedimientos de seguridad de los datos del titular de la tarjeta.	Si el personal no conoce sus responsabilidades de seguridad, las defensas y los procesos de seguridad que se han implementado pueden volverse ineficaces a causa de errores o acciones intencionales.
	12.6.b Revise los procedimientos y la documentación del programa de concienciación sobre seguridad y realice lo siguiente:	
12.6.1 Capacite al personal inmediatamente después de contratarlo y, al menos, una vez al año. ***Nota:*** *Los métodos pueden variar según el rol del personal y del nivel de acceso a los datos del titular de la tarjeta.*	**12.6.1.a** Verifique que el programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los empleados en lo que respecta a la concienciación (por ejemplo, carteles, cartas, notas, capacitación en línea, reuniones y promociones).	Si el programa de concienciación sobre seguridad no incluye sesiones de repaso periódicas, es posible los procesos y procedimientos de seguridad clave no se tengan en cuenta o se omitan, por lo que los recursos críticos y los datos del titular de la tarjeta podrían quedar expuestos.
	12.6.1.b Verifique que el personal concurra a la capacitación de la concienciación sobre seguridad al ser contratados y, al menos, una vez al año.	
	12.6.1.c Entreviste a un grupo de empleados para verificar que hayan realizado la capacitación de concienciación y que conozcan la importancia de la seguridad de los datos del titular de la tarjeta.	
12.6.2 Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa.	**12.6.2** Verifique que el programa de concienciación sobre seguridad les exija a los empleados realizar, al menos, una vez al año, una declaración escrita o electrónica de que leyeron y entendieron la política de seguridad de la información de la empresa.	Requerir un reconocimiento de los empleados por escrito o electrónico ayuda a asegurar que han leído y comprendido las políticas y los procesos de seguridad, y que están y estarán comprometidos con el cumplimiento de dichas políticas.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.7 Examine al personal potencial antes de contratarlo 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 potenciales miembros del personal considerados para ciertos puestos, como cajeros de un comercio —que solo tienen acceso a un número de tarjeta a la vez al realizar una transacción—, este requisito es solo una recomendación.*	**12.7** Consulte con la gerencia del departamento de Recursos Humanos y verifique que se realiza un control de los antecedentes de los posibles empleados (dentro de los límites de las leyes locales) antes de contratar a los posibles empleados que tendrán acceso a los datos del titular de la tarjeta o al entorno de los datos del titular de la tarjeta.	Investigar exhaustivamente los antecedentes de los posibles empleados que tendrán acceso a los datos del titular de la tarjeta antes de contratarlos reduce el riesgo del uso no autorizado de los PAN (números de cuenta principal) y de otros datos del titular de la tarjeta por parte de personas con antecedentes cuestionables o delictivos.
12.8 Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera:	**12.8** A través de la observación, la revisión de políticas y procedimientos y el análisis de documentos de apoyo, verifique que se implementen los procesos para administrar a los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera:	Si un comerciante o proveedor de servicios comparte datos del titular de la tarjeta con un proveedor de servicios, se aplican ciertos requisitos para garantizar que dichos proveedores de servicios protegerán siempre los datos. Algunos ejemplos de los diferentes tipos de proveedores de servicios incluyen a las instalaciones de almacenamiento en cinta de copia de seguridad, los proveedores de servicios gestionados, como las empresas de alojamiento web o los proveedores de servicios de seguridad, las entidades que reciben datos con fines de modelado de fraude, etc.
12.8.1 Mantener una lista de proveedores de servicios, incluida una descripción del servicio prestado.	**12.8.1** Verifique que se mantiene una lista de proveedores de servicios y que incluya una descripción del servicio prestado.	Rastrear a todos los proveedores de servicios identifica dónde se extiende el riesgo potencial hacia fuera de la organización.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.8.2 Mantenga un acuerdo por escrito en el que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. ***Nota:*** *La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.*	**12.8.2** Observe los acuerdos escritos y confirme que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.	El reconocimiento por parte de los proveedores de servicios deja constancia de su compromiso por mantener la debida seguridad de los datos del titular de la tarjeta que obtienen de sus clientes. La medida en que el proveedor de servicios es responsable de la seguridad de los datos del titular de la tarjeta dependerá del servicio en particular y del acuerdo entre el proveedor y la entidad evaluada. Junto con el Requisito 12.9, el objetivo de este requisito es procurar un nivel de entendimiento uniforme entre las partes con respecto a sus responsabilidades de las PCI DSS aplicables. Por ejemplo, el acuerdo puede incluir que se cumplan los requisitos correspondientes de las PCI DSS como parte del servicio prestado.
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios, que incluya una auditoría adecuada previa al compromiso.	**12.8.3** Verifique que las políticas y los procedimientos estén documentados e implementados, que incluyan una auditoría adecuada previa al compromiso con cualquier proveedor de servicios.	El proceso asegura que una organización examine de manera exhaustiva e interna cualquier contratación de un proveedor de servicios. Dicho proceso debe incluir un análisis de riesgos previo al establecimiento de una relación formal con el proveedor de servicios. Los objetivos y los procesos específicos de la auditoría varían según la organización. Algunos ejemplos de consideraciones son las prácticas de presentación de informes del proveedor, la notificación de violaciones y los procedimientos de respuesta ante incidentes, detalles sobre cómo se asignan las responsabilidades de las PCI DSS entre cada parte, de qué manera el proveedor valida el cumplimiento de las PCI DSS y qué evidencia presentarán, etc.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.8.4 Mantenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.	**12.8.4** Verifique que la entidad tenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.	Conocer el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios es útil para saber y asegurarse de que este cumple con los mismos requisitos a los que está sujeta su organización. Si el proveedor de servicios ofrece diversos servicios, este requisito se aplicará a los servicios prestados al cliente y a los servicios que se encuentren dentro del alcance de la evaluación de las PCI DSS del cliente. La información específica que conserve una entidad dependerá del tipo de acuerdo que tenga con el proveedor, el tipo de servicio, etc. El objetivo es que la entidad evaluada conozca los requisitos de las PCI DSS que deben cumplir sus proveedores.
12.8.5 Conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.	**12.8.5** Verifique que la entidad conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.	
12.9 ***Requisitos adicionales solo para los proveedores de servicios:*** Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. ***Nota:*** *La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.*	**12.9** ***Procedimientos de pruebas adicionales para los proveedores de servicios:*** Revise las políticas y los procedimientos del proveedor de servicio y observe las plantillas de los acuerdos escritos para verificar que el proveedor de servicios acepta, por escrito y ante el cliente, mantener los requisitos correspondientes de las PCI DSS en la medida en que el proveedor de servicios posea o, de otra manera, manipule, almacene, procese o transmita datos del titular de la tarjeta en nombre del cliente, o datos de autenticación confidenciales, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Junto con el Requisito 12.8.2, el objetivo de este requisito es procurar un nivel de entendimiento uniforme entre los proveedores de servicios y los clientes respecto de las responsabilidades correspondientes de las PCI DSS. El reconocimiento por parte de los proveedores de servicios deja constancia de su compromiso por mantener la debida seguridad de los datos del titular de la tarjeta que obtienen de sus clientes. Las políticas internas y los procedimientos del proveedor de servicios relacionados con su proceso de compromiso con el cliente y las plantillas utilizadas para los acuerdos por escrito deberán incluir el establecimiento de un reconocimiento de la PCI DSS aplicable a sus clientes. El método mediante el cual el proveedor de servicios proporciona el reconocimiento escrito debe establecerse entre el proveedor y los clientes.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.10 Implemente un plan de respuesta ante incidentes. Estar preparado para responder de inmediato ante una violación del sistema.	**12.10** Revise el plan de respuesta ante incidentes y los procedimientos relacionados para verificar que la entidad está preparada para responder inmediatamente ante una falla del sistema mediante lo siguiente:	Sin un exhaustivo plan de respuesta ante incidentes de seguridad debidamente diseminado, leído y comprendido por las partes responsables, la confusión y la falta de una respuesta unificada podrían crear períodos de inactividad más prolongados para el negocio, una exposición mediática innecesaria y nuevas responsabilidades legales.
12.10.1 Desarrolle el plan de respuesta ante incidentes que se implementará en caso de que ocurra una falla 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 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 ante incidentes de las marcas de pago.	**12.10.1.a** Verifique que el plan de respuesta ante incidentes incluya lo siguiente: • Las funciones, responsabilidades y estrategias de comunicación en caso de un riesgo que incluya como mínimo la notificación de las marcas de pago; • Procedimientos específicos de respuesta a incidentes. • Procedimientos de recuperación y continuidad comercial. • Procesos de 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 supuesto por operaciones comerciales con residentes de California en su base de datos). • La cobertura y respuestas de todos los componentes críticos del sistema; • Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.	El plan de respuesta a incidentes debe ser exhaustivo y contener todos los elementos clave para permitir que su empresa responda de manera efectiva en caso de un fallo en el sistema que pueda afectar los datos de titulares de tarjetas.
	12.10.1.b Entreviste al personal y revise la documentación de la muestra de un incidente o una alerta anteriormente informados para verificar que se hayan respetado los procedimientos y el plan de respuesta ante incidentes documentados.	

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.10.2 Revise y pruebe el plan, incluidos todos los elementos enumerados en el Requisito 12.10.1, al menos anualmente.	**12.10.2** Entreviste al personal y revise la documentación de las pruebas para verificar que el plan se prueba al menos anualmente, y que la prueba incluye todos los elementos enumerados en el Requisito 12.10.1.	Sin las pruebas apropiadas, es posible que se omitan pasos fundamentales, lo que podría generar una mayor exposición durante un incidente.
12.10.3 Designe a personal específico para que esté disponible las 24 horas al día, los 7 días de la semana para responder a las alertas.	**12.10.3** Mediante la observación, revise las políticas y entreviste al personal responsable para verificar que el personal designado esté siempre disponible (24 horas del día, los 7 días de la semana) para responder ante incidentes y que monitoreen la cobertura de cualquier evidencia de actividad no autorizada, detección de puntos de acceso inalámbricos no autorizados, alertas críticas de IDS (sistemas de intrusión-detección) o informes de cambios no autorizados en archivos de contenido o de sistemas críticos.	Sin un equipo de respuesta a incidentes capacitado y fácilmente disponible, podría producirse mayor daño para la red, además, los datos y sistemas críticos se pueden “contaminar” si los sistemas objetivo se manipulan indebidamente. Esto puede entorpecer el éxito de una investigación posterior al incidente.
12.10.4 Capacite adecuadamente al personal sobre las responsabilidades de respuesta ante fallas de seguridad.	**12.10.4** Mediante la observación, la revisión de las políticas y las entrevistas al personal responsable, verifique que el personal se capacite periódicamente en las responsabilidades ante fallas de seguridad.	
12.10.5 Incluya alertas de los sistemas de supervisión de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, *firewalls* y sistemas de supervisión de integridad de archivos.	**12.10.5** Mediante la observación y revisión de los procesos, verifique que, en el plan de respuesta ante incidentes, se incluya la supervisión y respuesta a las alertas de los sistemas de seguridad.	Estos sistemas de supervisión están diseñados para centrarse en el riesgo potencial para los datos, son críticos a la hora de ejecutar una acción para prevenir un fallo y se deben incluir en los procesos de respuesta a incidentes.
12.10.6 Elabore un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.	**12.10.6** Mediante la observación, la revisión de las políticas y las entrevistas al personal responsable, verifique que exista un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.	Incorporar las “lecciones aprendidas” en el plan de respuesta a incidentes ayuda a mantener el plan actualizado y a ser capaz de reaccionar ante las amenazas emergentes y las tendencias de seguridad.

Requisitos de la PCI DSS	Procedimientos de prueba	Guía
12.11 ***Requisitos adicionales solo para los proveedores de servicios:*** Realizar revisiones al menos cada tres meses para confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos. Las revisiones deben abarcar los siguientes procesos: • Revisiones del registro diario • Revisiones del conjunto de reglas de *firewall* • La aplicación de las normas de configuración a los nuevos sistemas • Respuesta a las alertas de seguridad • Procesos de gestión del cambio	**12.11.a** Revise las políticas y los procedimientos para verificar que los procesos se definen para revisar y confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos, y que las revisiones cubren: • Revisiones del registro diario • Revisiones del conjunto de reglas de *firewall* • La aplicación de las normas de configuración a los nuevos sistemas • Respuesta a las alertas de seguridad • Procesos de gestión del cambio **12.11.b** Entreviste al personal responsable y revise los registros de las revisiones para verificar que las revisiones se realizan por lo menos trimestralmente.	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* Confirmar regularmente que se siguen las políticas y procedimientos de seguridad proporciona una certeza de que los controles previstos están activos y que funcionan según lo previsto. El objetivo de estas revisiones no es volver a realizar otros requisitos de la PCI DSS, sino confirmar si los procedimientos se siguen como se esperaba.
12.11.1 ***Requisitos adicionales solo para los proveedores de servicios:*** Mantener la documentación del proceso de revisión trimestral para incluir: • Documentar los resultados de las revisiones • Revisión y cierre de los resultados por el personal asignado a la responsabilidad del programa de cumplimiento de la PCI DSS	**12.11.1** Revise la documentación de las revisiones trimestrales para verificar que incluyen: • Documentar los resultados de las revisiones • Revisión y cierre de los resultados por el personal asignado a la responsabilidad del programa de cumplimiento de la PCI DSS	***Nota:*** *Este requisito rige solo cuando la entidad evaluada es un proveedor de servicios.* La intención de estos controles independientes es confirmar si las actividades de seguridad se realizan de manera continua. Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de *firewall*, etc., para ayudar a la entidad a prepararse para la siguiente evaluación de la PCI DSS.

Anexo A: Requisitos adicionales de las PCI DSS

Este anexo contiene los requisitos adicionales de la PCI DSS para los diferentes tipos de entidades. Las secciones de este Anexo incluyen:

- Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de *hosting* compartido
- Anexo A2: Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana para conexiones de terminal de POS POI de tarjeta presente
- Anexo A3: Validación suplementaria de las entidades designadas

Se proporciona guía e información de aplicabilidad en cada sección.

Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido

Tal como se menciona en los Requisitos 12.8 y 12.9, todos los proveedores de servicios con acceso a los datos del titular de la tarjeta (incluidos los proveedores de *hosting* compartido) deben respetar las PCI DSS. Además, el Requisito 2.6 establece que los proveedores de *hosting* compartido deben proteger el entorno y los datos alojados de cada entidad. Por lo tanto, los proveedores de *hosting* compartido deben cumplir además con los requisitos de este Anexo.

Requisitos A1	Procedimientos de prueba	Guía
A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicios u otra entidad), según los puntos A.1.1 a A.1.4: Un proveedor de *hosting* debe cumplir estos requisitos, así como también las demás secciones pertinentes de la 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** En el caso específico de la evaluación de las PCI DSS de un proveedor de *hosting* compartido, verifique que los proveedores de *hosting* compartido protejan los datos y el entorno alojado de 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 los puntos de A.1.1 a A.1.4 a continuación:	*El Anexo A* de las PCI DSS está dirigido a los proveedores de *hosting* compartido que deseen ofrecerles a sus clientes comerciantes o proveedores de servicios un entorno de *hosting* que cumpla con las PCI DSS.
A.1.1 Asegúrese de que cada entidad solo implemente procesos que tengan acceso al entorno de datos del titular de la tarjeta 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.	Si se permite a un comerciante o proveedor de servicios ejecutar sus propias aplicaciones en el servidor compartido, se deberán ejecutar con la ID de usuario del comerciante o del proveedor de servicios y no, como un usuario con privilegios.

Requisitos A1	Procedimientos de prueba	Guía
A.1.2 Limite el acceso y los privilegios de cada entidad solo al entorno de sus propios datos del titular de la tarjeta.	**A.1.2.a** Verifique que la ID de usuario de cualquier proceso de aplicación no sea un usuario con privilegios (raíz/admin).	Para garantizar la restricción de los privilegios y accesos para que cada comerciante o proveedor de servicios acceda solo a su propio entorno, considere lo siguiente: 1. Privilegios de la ID de usuario de servidor web del comerciante o proveedor de servicios. 2. Privilegios otorgados para leer, escribir y ejecutar archivos. 3. Permisos otorgados para escribir en los archivos binarios del sistema. 4. Permisos otorgados a los archivos de registros del comerciante y del proveedor de servicios. 5. Controles para evitar que solo un comerciante o proveedor de servicios monopolice los recursos del sistema.
	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 la entidad no tengan acceso de escritura a los archivos binarios compartidos del sistema.	
	A.1.2.d Verifique que la visualización de las entradas del registro se restrinja a la entidad propietaria.	
	A.1.2.e Para asegurarse de que ninguna entidad monopoliza los recursos del servidor y se aproveche de las vulnerabilidades (por ejemplo, error, carrera y condiciones de reinicio que tienen como consecuencia, por ejemplo, desbordamientos de buffer), verifique que se apliquen las restricciones para el uso de estos recursos del sistema: • Espacio en disco • Ancho de banda • Memoria • CPU	
A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos del titular de la tarjeta de cada entidad y que cumplan con el Requisito 10 de las PCI DSS.	**A1.3** 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.	Los registros deben estar disponibles en un entorno de *hosting* compartido de manera tal que los comerciantes y los proveedores de servicio tengan acceso a registros específicos del entorno de datos de sus titulares de tarjetas y puedan revisarlos.

Requisitos A1	Procedimientos de prueba	Guía
A1.4 Habilite los procesos para que se realice una investigación forense oportuna en caso de que un comerciante o proveedor de servicios alojado corra riesgos.	**A1.4** Verifique que el proveedor de *hosting* compartido cuente con políticas escritas que especifiquen la realización de una investigación forense oportuna de los servidores relacionados en caso de riesgo.	Los proveedores de alojamiento compartido deben tener procesos que proporcionen respuestas rápidas y sencillas en caso de que sea necesaria una investigación la existencia de riesgos, hasta el nivel de detalle que sea necesario de manera que los detalles de un proveedor de servicios o de un comerciante individual.

Anexo A2: Requisitos de PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana para conexiones de terminal de POS POI de la tarjeta presente

Las entidades que usan SSL y TLS temprana para conexiones de terminal de POS POI deben trabajar para actualizarse a un protocolo de criptografía sólida lo antes posible. Además, la SSL y/o TLS temprana no deben ser introducidas en entornos en los que dichos protocolos no existen. Al momento de la publicación, las vulnerabilidades conocidas son difíciles de aprovechar en los terminales de pagos de POS POI. Sin embargo, las nuevas vulnerabilidades podrían surgir en cualquier momento, y corresponde a la organización mantenerse actualizada con las tendencias de vulnerabilidades y determinar si es o no susceptible a ataques conocidos.

Los requisitos de la PCI DSS directamente afectados son:

Requisito 2.2.3	Implementar funciones de seguridad adicionales para los servicios, protocolos o *daemons* requeridos que no se consideren seguros.
Requisito 2.3	Cifre todo el acceso administrativo que no sea de consola utilizando una criptografía sólida.
Requisito 4.1	Utilice criptografía y protocolos de seguridad sólidos para salvaguardar los datos confidenciales de los titulares de las tarjetas durante su transmisión a través de redes públicas abiertas.

SSL y TLS temprana no deberán utilizarse como un control de seguridad para cumplir estos requisitos, excepto en el caso de las conexiones de terminal de POS POI que se detallan en este anexo. Para apoyar a las entidades que trabajan para migrar de SSL/TLS temprana en terminales de POS POI, se incluyen las siguientes disposiciones:

- Las nuevas implementaciones de terminal de POS POI no deben utilizar SSL o TLS temprana como un control de seguridad.
- Todos los proveedores de servicios de terminales de POS POI deben ofrecer una oferta de servicios segura.
- Los proveedores de servicios que brinden soporte a las implementaciones de terminales de POS POI que utilizan SSL y/o TLS temprana deben tener un Plan de migración y de mitigación de riesgo formal implementados.
- Los terminales de POS POI en entornos de tarjeta presente que pueden ser verificadas por no ser susceptibles a cualquier ataque conocido para SSL y TLS temprana, **y los puntos de terminación SSL/TLS a los que se conectan,** pueden seguir utilizando estos como un control de seguridad.

Este Anexo solo se aplica a las entidades que utilizan SSL/TLS temprana como un control de seguridad para proteger los terminales de POS POI, incluidos los proveedores de servicios que proporcionan las conexiones a los terminales de POS POI.

Requisitos A2	Procedimientos de prueba	Guía

Requisitos A2	Procedimientos de prueba	Guía
A2.1 En los terminales de POI POS (en la ubicación del canal de aceptación de pago o del comerciante) que utilizan SSL o TLS temprana, la entidad debe: confirmar que los dispositivos no son susceptibles a las vulnerabilidades conocidas para estos protocolos. ***Nota:*** *El objetivo de este requisito es aplicarlo a la entidad con el terminal de POS POI, como el comerciante. Este requisito no está destinado a los proveedores de servicios que funcionan como puntos de conexión o finalización para estos terminales de POS POI. Los requisitos A2.2 y A2.3 se aplican a los proveedores de servicios de POS POI.*	**A2.1** *Para los terminales de POS POI que utilizan SSL y/o TLS temprana TLS,* confirme que la entidad tenga la documentación (por ejemplo, la documentación del proveedor, los detalles de configuración del sistema/red, etc.) que verifique que los dispositivos no son susceptibles a ninguna vulnerabilidad conocida para SSL/TLS temprana.	Los terminales de POS POI utilizados en entornos de tarjeta presente pueden seguir usando SSL/TLS temprana, cuando se puede mostrar que el terminal de POS POI no es susceptible a las vulnerabilidades conocidas actualmente. Sin embargo, SSL es una tecnología obsoleta y puede estar sujeta a más vulnerabilidades de seguridad en el futuro; por lo tanto, se recomienda encarecidamente que los terminales de POS POI se actualicen a un protocolo seguro lo antes posible. Si SSL/TLS temprana no es necesaria en el entorno, se debe desactivar el uso y el repliegue de estas versiones. Para obtener mayor orientación, consulte los actuales Suplementos de información de la PCI SSC sobre SSL/TLS temprana. ***Nota:*** *La provisión para terminales de POS POI que actualmente no es susceptible a vulnerabilidades se basa en los riesgos actuales conocidos. Los terminales de POS POI deberán actualizarse de inmediato si ingresan nuevas vulnerabilidades para las cuales sean susceptibles.*

Requisitos A2	Procedimientos de prueba	Guía
A2.2 ***Requisito solo para los proveedores de servicios:*** Todos los proveedores de servicios con puntos de conexión existentes a los terminales de POS POI, según lo indicado en el Requisito A2.1, que usan SSL o TLS temprana deben tener un Plan de migración y de Mitigación de riesgo formal implementado.	**A2.2** Revise el Plan de Migración y de mitigación del riesgo documentado para verificar que incluya: • Descripción del uso, incluidos los datos que se están transmitiendo, los tipos y el número de sistemas que utilizan y/o dan soporte a SSL/TLS temprana, el tipo de entorno; • Resultados de la evaluación de riesgos y controles de reducción de riesgos implementados; • Descripción de los procesos a monitorear para las nuevas vulnerabilidades asociadas con SSL/TLS temprana; • Descripción de los procesos de control de cambios que se implementan para garantizar que SSL/TLS temprana no se implementa en los nuevos entornos; • Descripción general del plan del proyecto de migración para reemplazar la SSL/TLS temprana en una fecha futura.	Los puntos de terminación de POS POI, incluidos pero sin limitarse a, los proveedores de servicios, tal como un adquirente o procesador adquirente, pueden continuar utilizando SSL/TLS temprana cuando se puede demostrar que el proveedor de servicios tiene controles en ejecución para mitigar el riesgo de admitir conexiones para el entorno del proveedor de servicios. El Plan de Mitigación y Migración de riesgos es un documento preparado por la entidad que detalla sus planes para migrar a un protocolo seguro, y también describe los controles que la entidad ha implementado para reducir el riesgo asociado con SSL/TLS temprana hasta que finalice la migración. Los proveedores de servicios deben comunicarles a todos los clientes que utilizan SSL/TLS temprana sobre los riesgos asociados con dicha utilización y sobre la necesidad de migrar a un protocolo seguro. Para obtener una mayor orientación, consulte los actuales Suplementos de información de la PCI SSC en SSL/TLS temprana sobre los Planes de Migración y de Mitigación de riesgos.
A2.3 ***Requisito solo para los proveedores de servicios:*** Todos los proveedores de servicios deben brindar una oferta de servicios segura.	**A2.3** Revise las configuraciones del sistema y la documentación de apoyo para verificar que el proveedor de servicios ofrece una opción de protocolo seguro para su servicio.	Los proveedores de servicios de admiten conexiones de SSL/TLS temprana para terminales de POS POI también deben brindar una opción de protocolo de seguridad. Para obtener mayor orientación, consulte los actuales Suplementos de información de la PCI SSC sobre SSL/TLS temprana.

Anexo A3: Validación suplementaria de las entidades designadas (DES)

Este Anexo se aplica únicamente a las entidades designadas por una marca de pago o adquirente que exige una validación adicional de los requisitos de la PCI DSS existentes. Ejemplos de las entidades a las que se podría aplicar este Anexo ***pueden*** incluir:

- Aquellas que almacenan, procesan y/o transmiten grandes volúmenes de datos del titular de la tarjeta,
- Las que proporcionan puntos de agregación a los datos del titular de la tarjeta, o
- Las que han sufrido brechas significativas o reiteradas de los datos del titular de la tarjeta.

Estos pasos de la validación suplementaria están destinados a proporcionar mayor certeza de que los controles de la PCI DSS se mantienen eficazmente y de manera continua a través de los procesos de validación habituales (BAU), y el aumento de la validación y la consideración del alcance.

Los pasos de validación adicionales en este documento están organizados en las siguientes áreas de control:

A3.1 *Implementar un programa de cumplimiento de la PCI DSS.*

A3.2 *Documentar y validar el alcance de la PCI DSS.*

A3.3 *Validar la PCI DSS se incorpora en las actividades habituales (BAU).*

A3.4 *Controlar y gestionar el acceso lógico al entorno de los datos del titular de la tarjeta.*

A3.5 *Identificar y responder a eventos sospechosos.*

Nota: *Algunos de los requisitos han definido marcos de tiempo (por ejemplo, al menos trimestralmente o cada seis meses) en el que se realizarán ciertas actividades. Para la evaluación inicial para este documento, no se requiere que una actividad se haya realizado para cada plazo durante el año anterior, si el asesor verifica:*

1) La actividad se llevó a cabo de acuerdo con el requisito aplicable dentro del marco de tiempo más reciente (es decir, el trimestre más reciente o seis meses), y

2) La entidad cuenta con políticas y procedimientos documentados para seguir realizando la actividad dentro del marco de tiempo definido.

Para los años siguientes después de la evaluación inicial, una actividad debe haber sido realizada para cada período de tiempo que se requiere (por ejemplo, una actividad trimestral debe haber sido realizada para cada uno de los cuatro trimestres del año anterior).

Nota: *La entidad estará obligada a someterse a una evaluación conforme a este Anexo* ***SOLO si así lo indica un adquirente o una marca de pago.***

Requisitos A3	Procedimientos de prueba	Guía
A3.1 Implementar un programa de cumplimiento de la PCI DSS		
A3.1.1 La gerencia ejecutiva deberá establecerá la responsabilidad de la protección de los datos del titular de la tarjeta y un programa de cumplimiento de la PCI DSS para incluir: • Responsabilidad general de mantener el cumplimiento de la PCI DSS • La definición de un estatuto para el programa de cumplimiento de la PCI DSS • Proporcionar actualizaciones a la gerencia ejecutiva y a la junta directiva sobre las iniciativas y los problemas de cumplimiento de la PCI DSS, incluidas las actividades de remediación, al menos anualmente ***Referencia de la PCI DSS:*** *Requisito 12*	**A3.1.1.a** Revise la documentación para verificar que la gerencia ejecutiva ha asignado la responsabilidad general de mantener el cumplimiento de la PCI DSS de la entidad. **A3.1.1.b** Revise el estatuto de la PCI DSS de la empresa para verificar que se describen las condiciones en las que se organiza el programa de cumplimiento de la PCI DSS. **A3.1.1.c** Revise las actas de reuniones y/o presentaciones de la gerencia ejecutiva y la junta directiva para garantizar que las iniciativas de cumplimiento de la PCI DSS y las actividades de remediación se comunican al menos anualmente.	La asignación de la gerencia ejecutiva de las responsabilidades de cumplimiento de la PCI DSS garantiza la visibilidad a nivel ejecutivo en el programa de cumplimiento de la PCI DSS y permite la oportunidad de hacer preguntas adecuadas para determinar la eficacia del programa e influir en las prioridades estratégicas. La responsabilidad general del programa de cumplimiento de la PCI DSS puede ser asignada a los roles individuales y/o a las unidades de negocio dentro de la organización.
A3.1.2 Un programa formal de cumplimiento de la PCI DSS debe estar implementado para incluir: • Definición de las actividades para mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Procesos anuales de evaluación de la PCI DSS • Los procesos para la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo al requisito) • Un proceso para realizar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones estratégicas comerciales ***Referencia de la PCI DSS:*** *Requisitos 1-12*	**A3.1.2.a** Revise las políticas y los procedimientos de seguridad de la información para verificar que los procesos estén definidos para realizar lo siguiente: • Mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Evaluaciones anuales de la PCI DSS • Validación continua de los requisitos de la PCI DSS • Análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas	Un programa de cumplimiento formal permite a una organización supervisar la salud de sus controles de seguridad, ser proactivo en el caso de que falle un control, y comunicar las actividades efectivamente y la situación de cumplimiento en toda la organización. El programa de cumplimiento de la PCI DSS puede ser un programa dedicado o parte de un programa de cumplimiento global y/o de gobierno, y deberá incluir una metodología bien definida que demuestra la evaluación coherente y eficaz. Ejemplo de las metodologías incluye: *Deming Circle of Plan-Do-Check-Act* (PDCA), ISO 27001, COBIT, DMAIC, y Six Sigma. *(continúa en la página siguiente)*

Requisitos A3	Procedimientos de prueba	Guía
	A3.1.2.b Entreviste al personal y observe las actividades de cumplimiento para verificar que los procesos definidos son implementados para lo siguiente: • Mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Evaluaciones anuales de la PCI DSS • Validación continua de los requisitos de la PCI DSS • Análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas	Mantener y supervisar el cumplimiento general de la PCI DSS de una organización incluye identificar las actividades que se realizarán a diario, semanal, mensual, trimestral o anual, y garantizar que estas actividades se llevan a cabo en consecuencia (por ejemplo, utilizar una autoevaluación de seguridad o metodología de PDCA). Los ejemplos de las decisiones comerciales estratégicas que se deberán analizar para los posibles impactos de la PCI DSS pueden incluir fusiones y adquisiciones, nuevas compras de tecnología, o nuevos canales de aceptación de pago.
A3.1.3 Los roles y las responsabilidades de cumplimiento de la PCI DSS deben definirse específicamente y asignarse formalmente a uno o más miembros del personal, incluido al menos lo siguiente: • Gestionar las actividades habituales de la PCI DSS • Gestionar las evaluaciones anuales de la PCI DSS • Gestionar la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo al requisito) • Gestionar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas ***Referencia de la PCI DSS:*** *Requisito 12*	**A3.1.3.a** Revise las políticas y procedimientos de la seguridad de la información y entreviste al personal para verificar que los roles y las responsabilidades están claramente definidos y que las tareas se asignan para incluir al menos lo siguiente: • Gestionar las actividades habituales de la PCI DSS • Gestionar las evaluaciones anuales de la PCI DSS • Gestionar la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo al requisito) • Gestionar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas	La definición formal de los roles y responsabilidades específicas de cumplimiento de la PCI DSS ayuda a asegurar la rendición de cuentas y la supervisión de los esfuerzos continuos de cumplimiento de la PCI DSS. Estas funciones se pueden asignar a un solo propietario o a varios propietarios de diferentes aspectos. La propiedad deberá ser asignada a las personas con la autoridad para tomar decisiones basadas en el riesgo y sobre las cuales descansa la responsabilidad para la función específica. Las tareas deberán definirse formalmente y los propietarios deberán ser capaces de demostrar una comprensión de sus responsabilidades y de la rendición de cuentas.
	A3.1.3.b Entreviste al personal responsable y verifique que estén familiarizados con el desempeño designado de sus responsabilidades y de cumplimiento de la PCI DSS.	

Requisitos A3	Procedimientos de prueba	Guía
A3.1.4 Proporcione capacitación sobre la seguridad de la información y/o la PCI DSS actualizada al menos anualmente para el personal con responsabilidades de cumplimiento de la PCI DSS (como se identifica en A3.1.3). ***Referencia de la PCI DSS:*** *Requisito 12*	**A3.1.4.a** Revise las políticas y procedimientos de seguridad de la información para verificar que la capacitación sobre la seguridad de la información y/o la PCI DSS se requiere por lo menos anualmente para cada rol con las responsabilidades de cumplimiento de la PCI DSS. **A3.1.4.b** Entreviste al personal y revise los certificados de asistencia u otros registros para verificar que el personal con responsabilidad de cumplimiento de la PCI DSS recibe capacitación de seguridad de la información similar y/o de la PCI DSS actualizada al menos anualmente.	El personal responsable del cumplimiento de la PCI DSS tiene necesidades específicas de capacitación que superan lo que normalmente se proporciona como capacitación de concienciación de seguridad general. Las personas con responsabilidades de cumplimiento con la PCI DSS deberán recibir capacitación especializada que, además de la concienciación general sobre seguridad de la información, se enfoque en los temas, las habilidades, los procesos o las metodologías específicos en materia de seguridad que deben seguirse para que esas personas realicen sus responsabilidades de cumplimiento de manera efectiva. Los terceros pueden ofrecer capacitación, por ejemplo, SANS o PCI SSC (Concienciación de PCI, PCIP, e ISA), las marcas de pago, y los adquirentes o la capacitación puede ser interna. El contenido de la capacitación deberá ser aplicable para la función de trabajo en particular y ser actual para incluir las últimas amenazas de seguridad y/o la versión de la PCI DSS. Para obtener una guía adicional sobre el desarrollo del contenido de capacitación de seguridad adecuada para los roles especializados, consulte el Suplemento de información de la PCI SSC sobre las *Mejores prácticas para la implementación de un Programa de concienciación de seguridad.*

Requisitos A3	Procedimientos de prueba	Guía
A3.2 Documentar y validar el alcance de la PCI DSS		
A3.2.1 Documentar y confirmar la precisión del alcance de la PCI DSS al menos trimestralmente y tras cambios significativos en el entorno del estudio. Como mínimo, la validación trimestral de alcance deberá incluir: • Identificar todas las redes en el alcance y los componentes del sistema • Identificar todas las redes en el alcance y la justificación para las redes que están fuera del alcance, incluidas las descripciones de todos los controles de segmentación implementados • La identificación de todas las entidades conectadas, por ejemplo, las entidades de terceros relacionadas con el acceso al entorno de los datos del titular de la tarjeta (CDE) ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS*	**A3.2.1.a** Revise los resultados documentados de las revisiones del alcance y entreviste al personal para verificar que se realizan las revisiones: • Al menos trimestralmente • Después de cualquier cambio significativo en el entorno **A3.2.1.b** Revise los resultados documentados de las revisiones de alcance trimestralmente para verificar que se realiza lo siguiente: • Identificación de todas las redes en el alcance y los componentes del sistema • Identificación de todas las redes fuera del alcance y la justificación de las redes por estar fuera del alcance, incluidas las descripciones de todos los controles de segmentación implementados • Identificación de todas las entidades conectadas, por ejemplo, entidades de terceros con acceso al CDE	La validación del alcance de la PCI DSS deberá realizarse con tanta frecuencia como sea posible para garantizar que el alcance de la PCI DSS se mantiene actualizado y alineado con los objetivos comerciales cambiantes.
A3.2.2 Determine el impacto del alcance de la PCI DSS para todos los cambios en los sistemas o redes, incluidas las adiciones de nuevos sistemas y nuevas conexiones de red. Los procesos deben incluir: • La realización de una evaluación formal de impacto de la PCI DSS • La identificación de los requisitos de la PCI DSS aplicables al sistema o red • Actualización del alcance de la PCI DSS en su caso • Cierre documentado de los resultados de la evaluación de impacto por parte del personal responsable (como se define en A3.1.3)	**A3.2.2** Revise la documentación de cambio y entreviste al personal para verificarlo para cada cambio en los sistemas o redes: • Se realizó una evaluación formal del impacto de la PCI DSS. • Se identificaron los requisitos de la PCI DSS aplicables a los cambios en la red o en los sistemas. • Se actualiza el alcance de la PCI DSS según sea apropiado para el cambio. • Se obtuvo y documentó el cierre por parte del personal responsable (como se define en A3.1.3).	Los cambios en los sistemas o redes pueden tener un impacto significativo en el alcance de la PCI DSS. Por ejemplo, los cambios en las reglas de *firewall* pueden poner a los segmentos en el alcance, o los nuevos sistemas pueden ser agregados al CDE que tiene que ser protegido adecuadamente. Se pueden realizar los procesos para determinar el impacto potencial que los cambios en los sistemas y redes pueden tener sobre el alcance de la PCI DSS de una entidad como parte de un programa de cumplimiento de la PCI DSS dedicado, o pueden caer bajo el programa de cumplimiento global y/o de gobierno de una entidad.

Requisitos A3	Procedimientos de prueba	Guía
Referencia de la PCI DSS: *Alcance de los requisitos de la PCI DSS; Requisitos 1-12*		

Requisitos A3	Procedimientos de prueba	Guía
A3.2.2.1 Al término de un cambio, se deben verificar todos los requisitos de la PCI DSS pertinente en todos los sistemas y redes nuevos o modificados y se debe actualizar la documentación, según sea el caso. Ejemplos de requisitos de la PCI DSS que deben ser verificados incluyen, pero no se limitan a: ▪ El Diagrama de una red se actualiza para reflejar los cambios. ▪ Los sistemas están configurados según las normas de configuración, con todas las contraseñas predeterminadas cambiadas y los servicios innecesarios deshabilitados. ▪ Los sistemas están protegidos con los controles requeridos, por ejemplo, la supervisión de la integridad de archivos (FIM), los antivirus, los parches, y el registro de auditoría. ▪ Verifique que los datos confidenciales de autenticación (SAD) no se almacenan y que el almacenamiento de todos los datos del titular de la tarjeta (CHD) se documenta e incorpora en la política y los procedimientos de retención de datos ▪ Los nuevos sistemas se incluyen en el proceso trimestral de análisis de vulnerabilidad. ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS; Requisito 1-12*	**A3.2.2.1** Para una muestra de los cambios en los sistemas y en la red, revise los registros de cambios, entreviste al personal y observe los sistemas/redes afectados para verificar que se implementaron los requisitos aplicables de la PCI DSS y que se actualizó la documentación como parte del cambio.	Es importante contar con procesos para analizar todos los cambios realizados para garantizar que todos los controles apropiados de la PCI DSS se aplican a cualquier sistema o red agregados al entorno del alcance debido a un cambio. La construcción de esta validación en los procesos de gestión de cambio ayuda a garantizar que los inventarios de los dispositivos y las normas de configuración se mantienen actualizados y los controles de seguridad se aplican donde sea necesario. Un proceso de gestión de cambio deberá incluir evidencia de apoyo que los requisitos de la PCI DSS se implementan o preservan mediante el proceso iterativo.

Requisitos A3	Procedimientos de prueba	Guía
A3.2.3 Los cambios en la estructura organizativa, por ejemplo, la fusión o la adquisición de empresas, el cambio o reasignación del personal encargado de los controles de seguridad, da lugar a una revisión formal (interna) del impacto del alcance de la PCI DSS y la aplicabilidad de los controles. ***Referencia de la PCI DSS:*** *Requisito 12*	**A3.2.3** Examinar las políticas y procedimientos para verificar que un cambio en la estructura organizativa da lugar a la revisión formal del impacto del alcance de la PCI DSS y la aplicabilidad de los controles.	La estructura y la gestión de una organización definen los requisitos y protocolos para las operaciones eficaces y seguras. Los cambios en esta estructura podrían tener efectos negativos en los controles y en los marcos existentes mediante la reasignación o la eliminación de los recursos que una vez apoyaron los controles de la PCI DSS o heredar nuevas responsabilidades que pueden no haber establecido controles implementados. Por lo tanto, es importante revisar nuevamente el alcance y los controles de la PCI DSS cuando hay cambios para garantizar que los controles están implementados y activos.
A3.2.4 Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación, al menos cada seis meses y después de cualquier cambio a los controles/métodos de segmentación. ***Referencia de la PCI DSS:*** *Requisito 11*	**A3.2.4** Examinar los resultados de la prueba de penetración más reciente para verificar que: • La prueba de penetración para verificar los controles de segmentación se realiza al menos cada seis meses y tras cualquier cambio en los controles/métodos de segmentación. • La prueba de penetración abarca todos los controles o métodos de segmentación implementados. • La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE.	Si la segmentación se utiliza para aislar las redes en el alcance de las redes fuera del alcance, los controles de segmentación deben verificarse mediante la prueba de penetración para confirmar que siguen funcionando según lo previsto y con eficacia. Las técnicas de las pruebas de penetración deberán seguir la metodología de penetración existente como se especifica en el Requisito 11 de la norma de la PCI DSS. Para obtener información adicional sobre la prueba de penetración efectiva, consulte el Suplemento de información de la PCI SSC sobre la *Guía de la prueba de penetración*.

Requisitos A3	Procedimientos de prueba	Guía
A3.2.5 Implemente una metodología de descubrimiento de datos para confirmar el alcance de la PCI DSS y para localizar todas las fuentes y ubicaciones de PAN en texto claro al menos trimestralmente y tras cambios significativos en el entorno o en los procesos del titular de tarjeta. La metodología de descubrimiento de datos debe tomar en consideración el potencial del PAN en texto claro para residir en los sistemas y en las redes fuera del CDE actualmente definido. ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS*	**A3.2.5.a** Revise la metodología de descubrimiento de datos documentada para verificar lo siguiente: • La metodología de descubrimiento de datos incluye procesos para identificar todas las fuentes y ubicaciones del PAN en texto claro. • La metodología toma en consideración el potencial del PAN en texto claro para residir en los sistemas y en las redes fuera del CDE actualmente definido. **A3.2.5.b** Revise los resultados de los recientes esfuerzos de descubrimiento de datos, y entreviste al personal responsable para verificar que el descubrimiento de datos se lleva a cabo por lo menos trimestralmente y tras cambios significativos en el entorno o en los procesos del titular de tarjeta.	La PCI DSS exige que, como parte del ejercicio de alcance, las entidades evaluadas deben identificar y documentar la existencia de todo el PAN en texto claro en sus entornos. La implementación de una metodología de descubrimiento de datos que identifica todas las fuentes y lugares de PAN en texto claro, y que tiene en cuenta la posibilidad de que el PAN en texto claro resida en los sistemas y en las redes fuera del CDE actualmente definido o en lugares inesperados dentro del CDE, por ejemplo, en un registro de errores o en un archivo de volcado de memoria, ayuda a garantizar que las ubicaciones previamente desconocidas del PAN en texto claro se detectan y se aseguran adecuadamente. Se puede realizar un proceso de descubrimiento de datos a través de una variedad de métodos, incluido, pero no limitado a: (1) software de descubrimiento de datos disponible en el mercado, (2) un programa interno de descubrimiento de datos, o (3) una búsqueda manual. Independientemente del método utilizado, el objetivo del esfuerzo es encontrar todas las fuentes y las ubicaciones del PAN en texto claro (no solo en el CDE definido).
A3.2.5.1 Garantice la eficacia de los métodos utilizados para el descubrimiento de los datos; por ejemplo, los métodos deben ser capaces de descubrir el PAN en texto claro en todos los tipos de componentes del sistema (por ejemplo, en cada sistema operativo o plataforma) y formatos de archivo en uso. Se debe confirmar la eficacia de los métodos de descubrimiento de datos por lo menos anualmente. ***Referencia de la PCI DSS:*** *Alcance de los*	**A3.2.5.1.a** Entreviste al personal y revise la documentación para verificar que: ▪ La entidad tiene un proceso implementado para probar la eficacia de los métodos utilizados para el descubrimiento de datos. ▪ El proceso incluye la verificación de los métodos que son capaces de descubrir el PAN en texto claro sobre todos los tipos de componentes del sistema y los formatos de archivo en uso. **A3.2.5.1.b** Revise los resultados de las pruebas de efectividad recientes para verificar que se confirma la eficacia de los métodos utilizados para el descubrimiento de datos, por lo menos anualmente.	Un proceso para poner a prueba la eficacia de los métodos utilizados para el descubrimiento de datos garantiza la integridad y la exactitud de la detección de los datos del titular de la tarjeta. Para la finalización, se deberá incluir al menos una muestra de los componentes del sistema, tanto en las redes dentro y fuera de alcance en el proceso de descubrimiento de datos. La precisión puede ser probada al colocar los PAN de prueba sobre una muestra de componentes del sistema y formatos de archivo en uso y confirmar que el método de descubrimiento de datos detectó el PAN de prueba.

Requisitos A3	Procedimientos de prueba	Guía
requisitos de la PCI DSS		
A3.2.5.2 Implemente procedimientos de respuesta a iniciar tras la detección del PAN en texto claro fuera del CDE para incluir: ▪ Procedimientos para determinar qué hacer si el PAN en texto claro se descubre fuera del CDE, incluidas su recuperación, eliminación segura y/o migración en el CDE definido actualmente, según sea el caso ▪ Procedimientos para determinar cómo los datos terminaron fuera del CDE ▪ Procedimientos para remediar las fugas de datos o las brechas de procesos que dieron lugar a que los datos queden fuera del CDE ▪ Procedimientos para identificar la fuente de los datos ▪ Procedimientos para identificar si datos de la pista se almacenan con el PAN	**A3.2.5.2.a** Revise los procedimientos de respuesta documentados para verificar que se definen e incluyen los procedimientos para responder a la detección del PAN en texto claro fuera del CDE: ▪ Procedimientos para determinar qué hacer si el PAN en texto claro se descubre fuera del CDE, incluidas su recuperación, eliminación segura y/o migración en el CDE definido actualmente, según sea el caso ▪ Procedimientos para determinar cómo los datos terminaron fuera del CDE ▪ Procedimientos para remediar las fugas de datos o las brechas de procesos que dieron lugar a que los datos queden fuera del CDE ▪ Procedimientos para identificar la fuente de los datos ▪ Procedimientos para identificar si datos de la pista se almacenan con el PAN	Después de documentar los procedimientos de respuesta que se siguen en el caso de que el PAN en texto claro se encuentre fuera del CDE ayuda a identificar las medidas de remediación necesarias y evitar fugas en el futuro. Por ejemplo, si el PAN fue encontrado fuera del CDE, el análisis se deberá realizar para (1) determinar si se ha guardado de forma independiente de otros datos (¿o si era parte de una pista completa?), (2) identificar el origen de los datos, y (3) identificar las brechas de control que dieron lugar a que los datos estén fuera del CDE.
	A3.2.5.2.b Entreviste al personal y examine los registros de las medidas de respuesta para que las actividades de remediación se realicen cuando se detecta el PAN en texto claro fuera del CDE.	
A3.2.6 Implemente mecanismos para detectar y prevenir que el PAN en texto claro salga del CDE a través de un canal, método o proceso no autorizado, incluida la generación de registros de auditoría y alertas. ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS*	**A3.2.6.a** Revise la documentación y observe los mecanismos implementados para verificar que los mecanismos están: • Implementados y funcionando activamente • Configurados para detectar y prevenir que el PAN en texto claro sale del CDE a través de un canal, método o proceso no autorizado • Generando registros y alertas tras la detección del PAN en texto claro que sale del CDE a través de un canal, método o proceso no autorizado	Mecanismos para detectar y prevenir la pérdida no autorizada del PAN en texto claro pueden incluir a las herramientas apropiadas, como las soluciones de prevención de pérdida de datos (DLP) y/o los procesos y procedimientos manuales adecuados. La cobertura de los mecanismos deberá incluir, sin carácter restrictivo, correos electrónicos, descargas a medios extraíbles y salidas a impresoras. El uso de estos mecanismos permite a una organización detectar y prevenir situaciones que pueden dar lugar a la pérdida de datos.
	A3.2.6.b Revise los registros de auditoría y las alertas, y entreviste al personal responsable para verificar que las alertas se investigan.	

Requisitos A3	Procedimientos de prueba	Guía
A3.2.6.1 Implemente los procedimientos de respuesta a iniciar tras la detección de intentos de eliminar el PAN en texto claro del CDE a través de un canal, método o proceso no autorizado. Los procedimientos de respuesta deben incluir: ▪ Procedimientos para la investigación oportuna de alertas por parte del personal responsable ▪ Procedimientos para remediar las fugas de datos o las brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos	**A3.2.6.1.a** Revise los procedimientos documentados de respuesta para verificar que los procedimientos para responder al intento de eliminación del PAN en texto claro del CDE a través de un canal, método o proceso no autorizado incluyen: ▪ Procedimientos para la investigación oportuna de alertas por parte del personal responsable ▪ Procedimientos para remediar las fugas de datos o las brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos	Los intentos de eliminar el PAN en texto claro a través de un canal, método o proceso no autorizado pueden indicar la mala intención de robar datos, o pueden ser las acciones de un empleado autorizado que no está consciente de o, simplemente, no sigue los métodos apropiados. La investigación oportuna de estos sucesos puede identificar dónde se necesita aplicar la remediación y ofrece información valiosa para ayudar a entender de dónde provienen las amenazas.
	A3.2.6.1.b Entreviste al personal y revise los registros de las medidas tomadas cuando se detecta que el PAN en texto claro sale del CDE a través de un canal, método o proceso no autorizado y verifique que se realizaron las actividades de remediación.	
A3.3 Validar la PCI DSS se incorpora en las actividades habituales (BAU)		
A3.3.1 Implemente un proceso para detectar y alertar de inmediato las fallas de control de seguridad críticas. Ejemplos de controles de seguridad críticos incluyen, pero no se limitan a: • *Firewalls* • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) ***Referencia de la PCI DSS:*** *Requisitos 1-12*	**A3.3.1.a** Revise las políticas y los procedimientos documentados para verificar que los procesos están definidos para detectar y alertar de inmediato sobre las fallas críticas de control de seguridad.	Sin procesos formales para la pronta detección (lo antes posible) y la alerta de las fallas de control de seguridad críticas, las fallas pueden pasar desapercibidas durante períodos prolongados y proporcionar a los atacantes tiempo suficiente para poner en riesgo los sistemas y robar datos sensibles del entorno de datos del titular de la tarjeta.
	A3.3.1.b Revise los procesos de detección y de alerta y entreviste al personal para verificar que los procesos se implementan para todos los controles de seguridad críticos, y que la falla de un control de seguridad crítico da lugar a la generación de una alerta.	

Requisitos A3	Procedimientos de prueba	Guía
A3.3.1.1 Responda a las fallas de los controles de seguridad críticos de manera oportuna. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: ▪ Restaurar las funciones de seguridad ▪ Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad ▪ Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz ▪ Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad ▪ Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad ▪ Implementar controles para prevenir que se vuelva a producir la causa de la falla ▪ Reanudar la supervisión de los controles de seguridad ***Referencia de la PCI DSS:*** *Requisitos 1-12*	**A3.3.1.1.a** Revise las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos se definen e implementan para responder a una falla en el control de seguridad, e incluya: ▪ Restaurar las funciones de seguridad ▪ Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad ▪ Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz ▪ Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad ▪ Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad ▪ Implementar controles para prevenir que se vuelva a producir la causa de la falla ▪ Reanudar la supervisión de los controles de seguridad	La evidencia documentada (por ejemplo, los registros dentro de un sistema de gestión de problemas) deberá apoyar los procesos y procedimientos implementados para responder a las fallas de seguridad. Además, el personal debe estar al tanto de sus responsabilidades en el caso de una falla. Las medidas y las respuestas a la falla deben capturarse en la evidencia documentada.
	A3.3.1.1.b Revise los registros para verificar que se documentan las fallas de control de seguridad para incluir: ▪ Identificación de las causas de la falla, incluida la causa raíz ▪ Duración (fecha y hora de inicio y fin) de la falla de seguridad ▪ Detalles de la remediación necesaria para abordar la causa raíz	

Requisitos A3	Procedimientos de prueba	Guía
A3.3.2 Revise las tecnologías de hardware y software por lo menos anualmente para confirmar si siguen cumpliendo los requisitos de la PCI DSS de la organización. (Por ejemplo, una revisión de las tecnologías que ya no reciben soporte del proveedor y y/o que ya no cumplen con las necesidades de seguridad de la organización.) El proceso incluye un plan para remediar las tecnologías que ya no cumplen con los requisitos de la PCI DSS de la organización, hasta e incluido el reemplazo de la tecnología, según sea el caso. ***Referencia de la PCI DSS:*** *Requisitos 2, 6*	**A3.3.2.a** Revise las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos se definen e implementan para revisar las tecnologías de hardware y software y confirmar si siguen cumpliendo con los requisitos de la PCI DSS de la organización. **A3.3.2.b** Revise los resultados de las recientes revisiones para verificar que las revisiones se realizan por lo menos anualmente. **A3.3.2.c** Para cualquier tecnología que se ha determinado que ya no cumple con los requisitos de la PCI DSS de la organización, verifique que un plan está implementado para remediar la tecnología.	Las tecnologías de hardware y software están en constante evolución, y las organizaciones deben ser conscientes de los cambios en las tecnologías que utilizan, así como las amenazas en evolución a esas tecnologías. Las organizaciones también deben ser conscientes de los cambios realizados por los proveedores de tecnología a sus productos o procesos de apoyo, para entender cómo estos cambios pueden afectar el uso de la organización de la tecnología. Las revisiones periódicas de las tecnologías que tienen una incidencia o influencia sobre los controles de la PCI DSS pueden ayudar con la compra, el uso y las estrategias de implementación, y garantizar que los controles que dependen de esas tecnologías sigan siendo eficaces.

Requisitos A3	Procedimientos de prueba	Guía
A3.3.3 Realizar revisiones por lo menos trimestralmente para verificar que se siguen las actividades de BAU. Las revisiones deben ser realizadas por el personal asignado al programa de cumplimiento de la PCI DSS (como se identifica en A3.1.3), e incluyen lo siguiente: • Confirmación de que se realizan todas las actividades de BAU (por ejemplo, A3.2.2, A3.2.6 y A3.3.1) • Confirmación de que el personal sigue las políticas de seguridad y los procedimientos operativos (por ejemplo, las revisiones del registro diario, las revisiones del conjunto de reglas de *firewall*, las normas de configuración para nuevos sistemas, etc.) • Documentar cómo se completaron las revisiones, incluido cómo se verificaron todas las actividades BAU como implementadas. • Se requiere la recopilación de la evidencia documentada para la evaluación anual de la PCI DSS • Revisión y cierre de los resultados por el personal asignado con la responsabilidad del programa de cumplimiento de la PCI DSS (como se identifica en A3.1.3) • Retención de registros y la documentación durante al menos 12 meses, que abarcan todas las actividades BAU ***Referencia de la PCI DSS:*** *Requisitos 1-12*	**A3.3.3.a** Revise las políticas y los procedimientos para verificar que los procesos se definen para la revisión y verificación de las actividades BAU. Verifique que los procesos incluyan lo siguiente: • Confirmar que todas las actividades BAU (por ejemplo, A3.2.2, A3.2.6 y A3.3.1) se realizan • Confirmar que el personal siga las políticas de seguridad y los procedimientos operativos (por ejemplo, las revisiones del registro diario, las revisiones del conjunto de reglas de *firewall*, las normas de configuración para nuevos sistemas, etc.) • Documentar cómo se completaron las revisiones, incluido cómo se verificaron todas las actividades BAU como implementadas • Recopilar la evidencia documentada según se requiera para la evaluación anual de la PCI DSS • La revisión y cierre de los resultados por parte de la gerencia ejecutiva con la responsabilidad asignada del gobierno de la PCI DSS • Mantener los registros y la documentación durante al menos 12 meses, que cubra todas las actividades BAU **A3.3.3.b** Entreviste al personal responsable y examine los registros de las revisiones para verificar que: • Las revisiones las realiza el personal asignado al programa de cumplimiento de la PCI DSS. • Las revisiones se realizan por lo menos trimestralmente.	La implementación de los controles de la PCI DSS en las actividades habituales es un método eficaz para garantizar que la seguridad se incluye como parte de las operaciones comerciales normales de manera continua. Por lo tanto, es importante que se realicen verificaciones independientes para garantizar que los controles BAU están activos y funcionan debidamente. La intención de estos controles independientes es revisar la evidencia que confirma que se realizan las actividades habituales. Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de *firewall*, etc., para ayudar a la entidad a prepararse para la siguiente evaluación de la PCI DSS.

Requisitos A3	Procedimientos de prueba	Guía
A3.4 Controlar y gestionar el acceso lógico al entorno de los datos del titular de la tarjeta		
A3.4.1 Revise las cuentas de usuario y los privilegios de acceso a los componentes del sistema en el alcance por lo menos cada seis meses para garantizar que las cuentas y el acceso de usuario siguen siendo adecuados en función al trabajo, y a lo autorizado. ***Referencia de la PCI DSS:*** *Requisito 7*	**A3.4.1** Entreviste al personal y revise la documentación de respaldo para verificar lo siguiente: • Las cuentas de usuario y los privilegios de acceso se revisan por lo menos cada seis meses. • Las revisiones confirman que el acceso es adecuado en función al trabajo, y que todo acceso está autorizado.	Los requisitos de acceso evolucionan con el tiempo a medida que las personas cambian roles o dejan la empresa, y a medida que cambian las funciones de trabajo. La gerencia debe revisar periódicamente, revalidar, y actualizar el acceso de los usuarios, según sea necesario, para reflejar los cambios en el personal, incluidas las funciones laborales de los terceros y de los usuarios.
A3.5 Identificar y responder a eventos sospechosos		
A3.5.1 Implementar una metodología para la identificación oportuna de los patrones de ataque y el comportamiento no deseado en todos los sistemas, por ejemplo, utilizar revisiones manuales coordinadas y/o herramientas de correlación de registro automatizadas que incluyan al menos lo siguiente: • Identificación de anomalías o actividades sospechosas, a medida que se producen • La emisión de alertas oportunas tras la detección de actividades sospechosas o anomalías para el personal responsable • Respuesta a las alertas de acuerdo con los procedimientos documentados de respuesta ***Referencia de la PCI DSS:*** *Requisitos 10, 12*	**A3.5.1.a** Revise la documentación y entreviste al personal para verificar que se define y se implementa una metodología para identificar los patrones de ataque y un comportamiento no deseado en todos los sistemas de manera oportuna, y que incluya lo siguiente: • Identificación de anomalías o actividades sospechosas, a medida que se producen • Emisión de alertas oportunas para el personal responsable • Respuesta a las alertas de acuerdo con los procedimientos documentados de respuesta **A3.5.1.b** Revise los procedimientos de respuesta a incidentes y entreviste al personal responsable para verificar que: • El personal de turno recibe alertas oportunas. • Se responde a las alertas según los procedimientos de respuesta documentados.	La capacidad de identificar patrones de ataque y un comportamiento no deseado en todos los sistemas es fundamental en la prevención, detección, o minimizar el impacto de los riesgos para los datos. La presencia de los registros en todos los entornos permite el rastreo, la alerta y el análisis cuando algo no funciona bien. Determinar la causa de un riesgo es muy difícil, si no imposible, sin un proceso para corroborar la información de los componentes del sistema críticos, y los sistemas que realizan funciones de seguridad, como *firewalls*, IDS/IPS, y los sistemas de supervisión de integridad de archivos (FIM). Por lo tanto, se deberá recoger, correlacionar y mantener los registros de todos los componentes del sistema críticos que realizan funciones de seguridad. Esto podría incluir el uso de productos de software y metodologías de servicios para proporcionar análisis, alertas y presentación de informes en tiempo real, como la información de seguridad y la gestión de eventos (SIEM), la supervisión de la integridad de archivos (FIM), o la detección de cambios.

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 la *columna de guía* 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.

   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 de red interna; (2) filtrado de dirección IP o dirección MAC y (3) contraseñas de un solo uso.

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.*

Definición y número de requisito:

	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: *8.1.1 ¿Se identifican todos los usuarios con una ID de usuario exclusiva antes de permitirles el acceso a los componentes del sistema y a los datos del titular de la tarjeta?*

	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 va a requerir que todos los usuarios inicien sesión en los servidores utilizando sus cuentas de usuario normales, y luego utilizar el comando "sudo" para ejecutar cualquier comando administrativo. Esto permite el uso de los privilegios de la cuenta "raíz" para ejecutar los comandos predefinidos que sudo registra en el registro de seguridad. De esta manera, se puede realizar un seguimiento de las acciones de cada usuario mediante la cuenta SU, sin necesidad de compartir con los usuarios la contraseña "raíz".*
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 sudo está configurado correctamente utilizando un archivo "sudoers", que solo los comandos predefinidos pueden ser ejecutados por los usuarios especificados, y que todas las actividades realizadas por esas personas que usan sudo están conectadas para identificar a la persona que*

		realiza las acciones utilizando los privilegios de "raíz".
6. Mantenimiento	Defina los procesos y controles que se aplican para mantener los controles de compensación.	*La empresa XYZ documenta los procesos y procedimientos para asegurarse de que la configuración SU no se cambie, modifique ni elimine para que los usuarios ejecuten comandos raíz sin que se los pueda identificar, rastrear o registrar.*

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